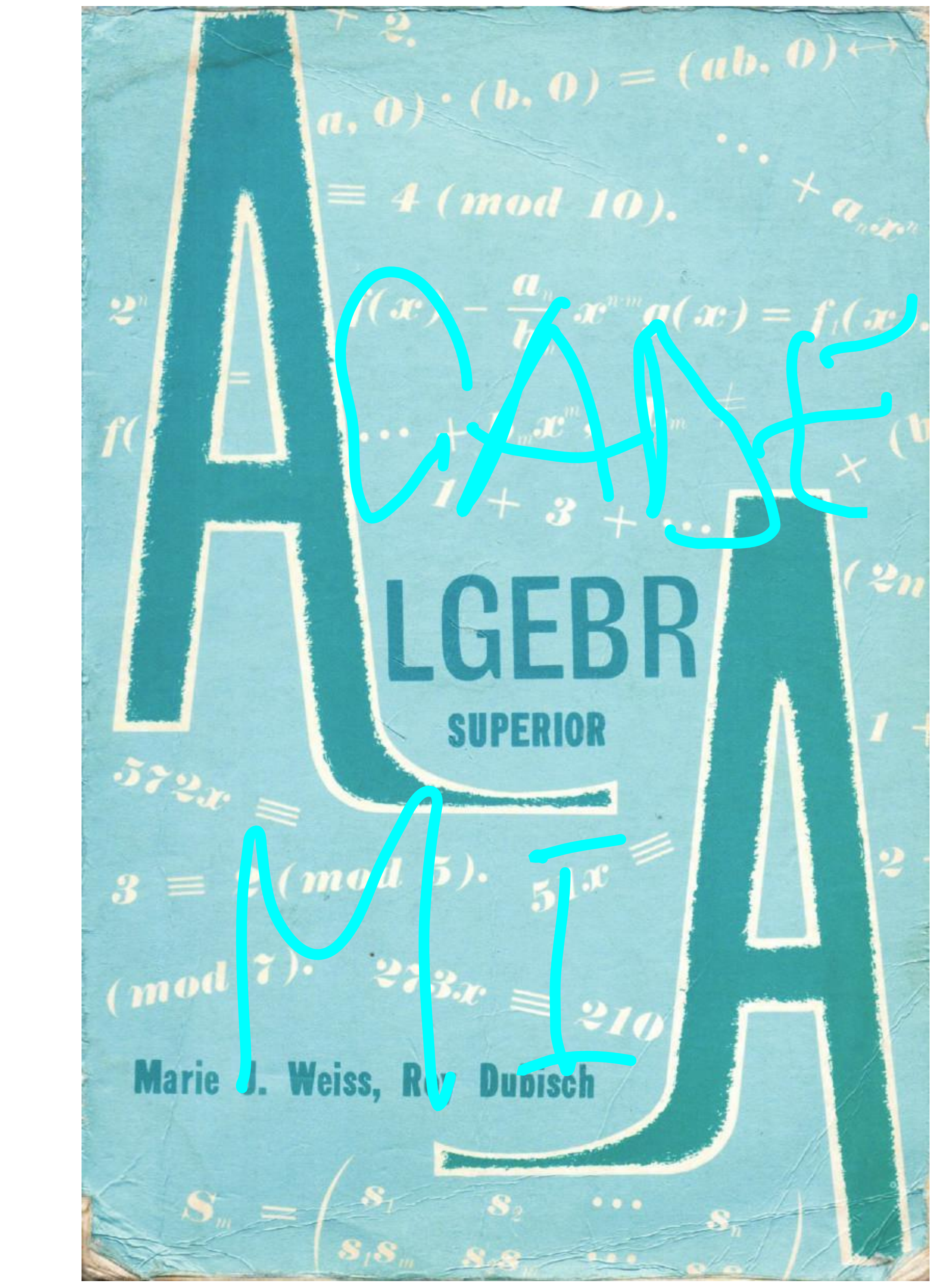
Este libro, es una revisión de la edición original escrita por Marie Weiss, y presenta una introducción al álgebra abstracta. Abarca los aspectos elementales más importantes de la materia: dominios enteros, anillos, campos, grupos, espacios vectoriales y matrices. Al preparar la revisión, el Profesor Dubisch conservó la organización y el espíritu del texto original. Sin embargo, agregó muchas ilustraciones constructivas y explícitas de las definiciones y aumentó considerablemente el número de ejercicios. Así mismo, con la adición de dos capítulos (6 y 7), se cubrieron tópicos como la independencia y dependencia lineal de vectores, los productos internos de vectores y el concepto de base y dimensión de un espacio vectorial que se habían omitido con anterioridad. Se evitaron las explicaciones sofisticadas y se usaron ejemplos sencillos para ilustrar los conceptos presentados.

El texto proporciona una transición suave y gradual de los cursos especiales para resolver problemas a la deducción postulatoria, proporcionando al estudiante una base sólida para efectuar trabajos posteriores en otros campos de las matemáticas.



Algebra Superior

MARIE J. WEISS
Ex Profesora de Matemáticas
Newcombe College, Tulane University, E. U. A.

ROY DUBISCH
Profesor de Matemáticas
Universidad de Wáshington, E. U. A.



EDITORIAL LIMUSA - WILEY, S. A.
MEXICO 1967

Título de la obra en inglés
HIGHER ALGEBRA FOR THE UNDERGRADUATE
Versión autorizada al español de la segunda edición
publicada por JOHN WILEY & SONS, INC., N. Y., E. U. A.
Derechos reservados por
© 1949, 1962. JOHN WILEY & SONS, INC.

Versión española:
JOSÉ HERNÁN PÉREZ CASTELLANOS,
Ingeniero Industrial.
Profesor de Matemáticas de la Escuela Superior de Ingeniería Mecánica y Eléctrica del Instituto Politécnico Nacional de México.

Revisión:
Físico, RAMÓN CORTÉS BARRIOS,
Profesor e investigador del Instituto Politécnico Nacional de México.
Profesor de Matemáticas de la Facultad de Ciencias de la Universidad Nacional Autónoma de México.

Derechos reservados en lengua española:
© 1967, EDITORIAL LIMUSA-WILEY, S. A.
Arcos de Belem núm. 75, México 1, D. F.
Miembro de la Cámara Nacional de la Industria Editorial, Reg. núm. 121.

Primera edición: 1967

Impreso en México
Printed in Mexico

Prólogo a la segunda edición en inglés

Al preparar la segunda edición de *Higher Algebra for the Undergraduate*, traté de conservar la organización y el espíritu de este excelente libro de texto. Sin embargo, hice un gran número de ligeros cambios en beneficio de la claridad y la corrección y algunos otros cambios de mayor trascendencia para proporcionar un panorama más amplio de las ideas básicas del álgebra abstracta elemental.

Entre las modificaciones más importantes se encuentras las siguientes:

1. Se introdujeron muchas ilustraciones constructivas y explícitas de las definiciones.

2. El número de ejercicios se incrementó en un 40%. Algunos de los ejercicios agregados son sencillos y los aumenté donde consideré que se necesitaban, pero otros son problemas más difíciles que se presentan para poner a prueba a los mejores estudiantes.

3. Antes de presentar temas no conocidos, se agregó material para estimular los conocimientos del estudiante (por ejemplo, los enteros negativos).

4. Para facilitar su identificación, todos los términos técnicos, introducidos ahora, se escribieron con letra cursiva.

5. Se actualizaron las referencias.

6. Se agregó al capítulo 4 una sección sobre dominios enteros ordenados y al capítulo 9 una sección sobre automorfismos de campos. (La última sección proporciona una introducción natural al estudio posterior de la moderna teoría de Galois.)

7. Probablemente, el cambio más importante es la renovación casi completa del capítulo 6, "Matrices sobre un campo". Este capítulo se reemplazó por dos: el capítulo 6 ahora se titula "Vectores y matrices" y el capítulo 7 actualmente denominado "Sistemas de ecuaciones lineales".

Estos nuevos capítulos incluyen tópicos como la independencia y dependencia lineal de vectores, el producto interno de vectores y el concepto de base y dimensión de un espacio vectorial (considerado como un conjunto de n-adas sobre un campo) que se omitieron en la edición anterior. Esta parte de la revisión está de acuerdo con la tendencia actual de enseñar más álgebra lineal al nivel de enseñanza superior.

Roy Dubisch

Seattle, Wáshington
Octubre 15, 1961

CONTENIDO

1 Enteros

1 · ENTEROS POSITIVOS

Los primeros símbolos matemáticos aprendidos por todos son los correspondientes a los enteros positivos: $1, 2, 3, \cdots$; a los cuales, frecuentemente se les da el nombre de *números naturales*. Sus propiedades son conocidas por todos y las enlistaremos sistemáticamente. No es nuestro propósito desarrollar estas propiedades a partir de un número mínimo de hipótesis y términos indefinidos, sino hacer una lista de esas leyes y propiedades que son tan familiares al estudiante y usarlas como una definición característica de los enteros positivos.

Las operaciones conocidas, en relación con los enteros positivos, son las de adición y multiplicación; es decir, para todo par de enteros positivos a, b, sabemos qué significan la suma de $a + b$ y el producto ab y que la suma y el producto también son enteros positivos. El hecho de que la suma y el producto de cualquier par de enteros positivos también sean enteros positivos, frecuentemente se expresa diciendo que el conjunto de los enteros positivos es *cerrado* bajo la adición y la multiplicación. Como es bien sabido, los enteros positivos $a, b, c, \cdots$ obedecen las siguientes leyes que gobiernan estas operaciones:

La ley conmutativa
para la adición $a + b = b + a,$
para la multiplicación $ab = ba.$

La ley asociativa
para la adición $a + (b + c) = (a + b) + c,$
para la multiplicación $a(bc) = (ab)c.$

La ley distributiva $a(b + c) = ab + ac.$

Por ejemplo, $2 + 3 = 5 = 3 + 2$; $2 \cdot 3 = 6 = 3 \cdot 2$; $2 + (3 + 4 = 2 + 7 = 9$ y, también, $(2 + 3) + 4 = 5 + 4 = 9$; $2(3 \cdot 4) = 2 \cdot 12 = 24$ y, también, $(2 \cdot 3)4 = 6 \cdot 4 = 24$; $2(3 + 4) = 2 \cdot 7 = 14$ y también, $2 \cdot 3 + 2 \cdot 4 = 6 + 8 = 14$.

Ahora pueden determinarse muchas otras propiedades de los enteros positivos con base en las propiedades antes establecidas. Por ejemplo, en ocasiones se da el nombre de ley distributiva *izquierda* a la ley distributiva $a(b + c) = ab + ac$ y puede establecerse la ley distributiva *derecha*

$$(b + c)a = ba + ca.$$

Aplicando sucesivamente la ley conmutativa para la multiplicación, la ley distributiva izquierda y, una vez más, la ley conmutativa para la multiplicación, se tiene $(b + c)a = a(b + c) = ab + ac = ba + ca$.

Puede darse una ilustración de un sistema en el cual no se cumplen algunas de estas leyes, definiendo arbitrariamente una adición y una multiplicación para los enteros positivos, de la manera siguiente: Denotemos la nueva adición por $\oplus$ y la nueva multiplicación por $\odot$. Sea $a \oplus b = 2a$ y $a \odot b = 2ab$, donde $2a$ y $2ab$ denotan los resultados de la multiplicación ordinaria. Entonces

$$b \oplus a = 2b, \quad b \odot a = 2ba, \quad a \oplus (b \oplus c) = a \oplus 2b = 2a,$$
$$(a \oplus b) \oplus c = 2a \oplus c = 4a, \quad a \odot (b \odot c) = a \odot 2bc = 4abc,$$
$$(a \odot b) \odot c = 2ab \odot c = 4abc, \quad a \odot (b \oplus c) = a \odot 2b = 4ab,$$
$$(a \odot b) \oplus (a \odot c) = 2ab \oplus 2ac = 4ab.$$

Nótese que las leyes conmutativa y asociativa no se cumplen para la adición, pero sí para la multiplicación ¿Existen dos leyes distributivas en este sistema?

Ejercicios

1. Reducir el primer miembro de las siguientes igualdades al segundo miembro, aplicando sucesivamente una ley asociativa, conmutativa o distributiva:

a. $(3 + 5) + 6 = 3 + (5 + 6)$. b. $1 + 5 = 5 + 1$.
c. $2(3 \cdot 5) = (2 \cdot 3)5$. d. $2(3 \cdot 5) = 5(2 \cdot 3)$.
e. $6(8 + 4) = 4 \cdot 6 + 6 \cdot 8$. f. $6(8 \cdot 4) = (4 \cdot 6)8$.
g. $3(7 + 5) = 5 \cdot 3 + 7 \cdot 3$. h. $5(6 + 3) = 3 \cdot 5 + 5 \cdot 6$.
i. $6(5 \cdot 3) = (3 \cdot 6)5$. j. $4 \cdot 6 + 7 \cdot 4 = 4(7 + 6)$.
k. $a[b + (c + d)] = (ab + ac) + ad$.
l. $a[b(cd)] = (bc)(ad)$. m. $a[b(cd)] = (ab)(cd)$.
n. $(ad + ca) + ag = a[(g + c) + d]$.

2. Determinar si las operaciones $\oplus$ y $\odot$ para los enteros positivos x, y, definidas en la forma que sigue, obedecen las leyes conmutativa, asociativa y distributiva:

a. $x \oplus y = x + 2y$, $x \odot y = 2xy$. b. $x \oplus y = xy$, $x \odot y = x + y$.
c. $x \oplus y = x + y^2$, $x \odot y = xy^2$. d. $x \oplus y = 2(x + y)$, $x \odot y = 2xy$.
e. $x \oplus y = x^2 + y^2$, $x \odot y = x^2y^2$.

2 · PROPIEDADES ADICIONALES

A continuación, se enlistarán algunas propiedades adicionales de los enteros positivos. Obsérvese que el entero positivo 1 es el único entero positivo tal que $1 \cdot a = a$, para todo entero positivo a. Se dice que 1 es una *identidad* para la multiplicación. Asimismo, se cumplen las siguientes leyes de *cancelación* para la adición y la multiplicación:

1. Si a, b y x son enteros positivos y $a + x = b + x$, entonces $a = b$.
2. Si a, b y x son enteros positivos y $ax = bx$, entonces $a = b$.

Además, para cualquier par de enteros positivos a y b, $a = b$, o bien, existe un entero positivo x tal que $a + x = b$, o bien existe un entero positivo y tal que $a = b + y$, y solamente se cumple una de estas alternativas. Por ejemplo, si $a = 2$ y $b = 2$, $a = b$; si $a = 2$ y $b = 3$, $2 + 1 = 3$; si $a = 3$ y $b = 2$, $3 = 2 + 1$.

A partir de estas relaciones alternativas entre dos enteros positivos, podemos definir las *desigualdades*. Si a, b y x son enteros positivos tales que $a + x = b$, se escribe $a < b$ (leer a menor que b) y $b > a$ (leer b mayor que a). Por tanto, $2 < 3$ y $3 > 2$ puesto que $2 + 1 = 3$. De aquí que, para cualquier par de enteros positivos, se tienen las siguientes alternativas mutuamente exclusivas —$a = b$, o $a < b$, o $a > b$— y se ha establecido una *relación de orden* entre cualquier par de enteros positivos. Con base en la definición anterior, pueden probarse las propiedades conocidas de las desigualdades para los enteros positivos:

1. Si $a < b$ y $b < c$, entonces $a < c$.
2. Si $a < b$, entonces $a + c < b + c$.
3. Si $a < b$, entonces $ac < bc$.

Por ejemplo, si $a < b$ y $b < c$, entonces existen los enteros positivos x y y tales que $a + x = b$ y $b + y = c$. Entonces $(a + x) + y = a + (x + y) = c$ y, puesto que $x + y$ es un entero positivo, $a < c$.

Ejercicios

1. Probar que, si a, b y c son enteros positivos y $a < b$, entonces $a + c < b + c$.
2. Probar que, si a, b y c son enteros positivos y $a < b$, entonces $ac < bc$.
3. Probar que, si a, b, c y d son enteros positivos, $a < b$ y $c < d$, entonces $a + c < b + d$.

3 · INDUCCION FINITA

Ahora llegamos a la última propiedad importante de los enteros positivos que se discutirá. Esta propiedad nos permitirá efectuar demostraciones por el método conocido como *inducción finita* o *inducción matemática*.

Postulado de la inducción finita

Un conjunto S de enteros positivos con las siguientes *dos* propiedades, contiene *todos* los enteros positivos:

1. El conjunto S contiene el entero positivo 1.
2. Si el conjunto S contiene el entero positivo k, contiene el entero positivo $k + 1$.

Este postulado se aplica para probar ciertas proposiciones relacionadas con los enteros positivos. Se dice que la demostración se realiza por inducción finita.

Primer método de demostración por inducción finita

Sea $P(n)$ una proposición definida para todo entero positivo n. Si $P(1)$ es verdadera y si $P(k + 1)$ es verdadera siempre que $P(k)$ sea verdadera, entonces $P(n)$ es verdadera para todos los enteros positivos n.

La demostración es inmediata de acuerdo con el postulado de la inducción finita. Considérese el conjunto S de enteros positivos para los cuales la proposición $P(n)$ es verdadera. Por hipótesis, contiene el entero positivo 1 y el entero positivo $k + 1$ siempre que contenga el entero positivo k. De aquí que el conjunto S contiene todos los enteros positivos.

EJEMPLO. Sea la potencia a^n, donde n es un entero positivo, definida de la manera siguiente: $a^1 = a$, $a^{k+1} = a^k \cdot a$. Probar que $(ab)^n = a^n b^n$.

Si $n = 1$, de acuerdo con la definición, $(ab)^1 = ab = a^1 b^1$. Supóngase que esta ley de los exponentes se cumple para $n = k$: $(ab)^k = a^k b^k$. Entonces, por definición, $(ab)^k(ab) = (ab)^{k+1}$ y, de acuerdo con el supuesto, $(ab)^k(ab) = (a^k b^k)(ab)$. Aplicando las leyes asociativa y conmutativa al segundo miembro de la última igualdad y según la definición, se tiene $(ab)^k(ab) = (a^k a)(b^k b) = a^{k+1} b^{k+1}$, lo que quería demostrarse. Por lo tanto, esta ley de los exponentes es verdadera para todos los enteros positivos n.

Intimamente relacionado con el postulado de la inducción finita se encuentra el *principio del buen orden:* En todo conjunto no vacío, de enteros postivos, existe un entero positivo más pequeño. Este principio puede probarse a partir del postulado de la inducción finita.* Aplicaremos este principio para establecer el

Segundo método de demostración por inducción finita

Sea $P(n)$ una proposición definida para todo entero positivo n. Si $P(1)$ es verdadera y si, para todo m, $P(m)$ es verdadera siempre que $P(k)$ sea verdadera para todos los enteros positivos $k < m$, entonces $P(n)$ es verdadera para todos los enteros positivos n.

Sea S el conjunto de enteros positivos para los cuales $P(n)$ es falsa. Si S no es vacío contendrá un entero positivo menor m. Nótese que $m \neq 1$, puesto que, por hipótesis, $P(1)$ es verdadera. De aquí que, para todos los enteros positivos $k < m$, $P(k)$ es verdadera. Entonces, a partir de la hipótesis de inducción, se tiene que $P(m)$ es verdadera, pero m está en el conjunto S. Por lo tanto, el conjunto S es vacío.

Ejercicios

Probar por inducción finita para todos los enteros positivos n.

1. Aplicar la definición dada en el ejemplo anterior para probar las leyes siguientes:

   a. $1^n = 1$. b. $a^m a^n = a^{m+n}$ c. $(a^m)^n = a^{mn}$.

2. $4 + 8 + 12 + \cdots + 4n = 2n(n + 1)$.
3. $3 \cdot 6 + 6 \cdot 9 + 9 \cdot 12 + \cdots + 3n(3n + 3) = 3n(n + 1)(n + 2)$.
4. $6 \cdot 1^2 + 6 \cdot 2^2 + 6 \cdot 3^2 + \cdots + 6n^2 = n(n + 1)(2n + 1)$.
5. $3 \cdot 1 \cdot 2 + 3 \cdot 2 \cdot 3 + 3 \cdot 3 \cdot 4 + \cdots + 3n(n + 1) = n(n + 1)(n + 2)$.
6. Probar los siguientes teoremas por inducción finita.

   a. $1 \leq n$ para todos los enteros positivos n.
   b. Si h y k son dos enteros positivos cualesquiera tales que $h < k + 1$, entonces $h \leq k$.
   c. Si m es un entero positivo cualquiera, entonces no existe entero positivo n tal que se cumpla $m < n < m + 1$.

* La demostración puede encontrarse en el libro *An Introduction to the Foundations and Fundamental Concepts of Mathematics* por H. Eves y C. V. Newsom, Nueva York, Rinehart & Co., 1958; o en *Foundations of Analysis*, p. 13, por E. Landau, Nueva York, Chelsea Book Co., 1951.

4 · RESUMEN

A continuación, como una referencia, se hará una lista de las propiedades de los enteros positivos que los caracterizan completamente. Estas propiedades pueden usarse como un conjunto de postulados para los enteros positivos.

El sistema de los enteros positivos tiene las propiedades siguientes:

1. El conjunto de enteros positivos es cerrado bajo las dos operaciones, adición y multiplicación. Estas operaciones obedecen las leyes conmutativa, asociativa y distributiva.
2. El entero positivo 1 tiene la propiedad $1 \cdot a = a$ para todo entero positivo a.
3. Se cumplen las leyes de cancelación. Si a, b y x son enteros positivos:

   i. Si $a + x = b + x$, entonces $a = b$.
   ii. Si $ax = bx$, entonces $a = b$.

4. Para cualquier par de enteros positivos a y b, se tiene $a = b$, o existe un entero positivo x tal que $a + x = b$, o existe un entero positivo y tal que $a = b + y$, y solamente se cumple una de estas alternativas.
5. Se cumple el postulado de la inducción finita.

5 · ENTEROS

Estamos familiarizados con el hecho de que, dados dos enteros positivos a y b, no siempre podemos encontrar un entero positivo x tal que $a + x = b$. Este estado inaceptable de cosas se remedió hace mucho tiempo mediante la introducción de los enteros negativos y el cero para construir el sistema de los enteros. Sin embargo, en lugar de suponer las propiedades de los enteros, se definirán los enteros en términos de los enteros positivos y las operaciones con enteros en términos de las operaciones con enteros positivos. Por tanto, podrán establecerse las propiedades de los enteros con base en las propiedades de los enteros positivos. Para hacer lo anterior, consideremos pares de enteros positivos tales como $(2, 1)$, $(1, 2)$, etc. Se definirá la igualdad, la adición y la multiplicación de estas parejas en tal forma que, por ejemplo, las parejas iguales a $(a + x, a)$ se comportarán de manera muy semejante a $(a + x) - a = x$, y las parejas iguales a $(a, a + x)$ se comportarán de modo muy semejante a $a - (a + x) = -x$.

Esta es la motivación para nuestras consideraciones. A continuación empecemos con un tratamiento formal de los símbolos (a, b), donde a y b son enteros positivos.

Definición de igualdad

La igualdad $(a, b) = (c, d)$ se cumple si y solamente si $a + d = b + c$. Aunque éste no es el concepto ordinario de igualdad, como identidad, se demostrará que tiene las propiedades usuales de la igualdad.

Teorema 1. *La igualdad* $(a, b) = (c, d)$ *es:*

1. *Reflexiva:* $(a, b) = (a, b)$.
2. *Simétrica: si* $(a, b) = (c, d)$, *entonces* $(c, d) = (a, b)$.
3. *Transitiva: si* $(a, b) = (c, d)$ *y si* $(c, d) = (e, f)$, *entonces* $(a, b) = (e, f)$.

Estas propiedades se demuestran rápidamente a partir de la definición de igualdad y las propiedades de los enteros positivos. Puesto que $a + b = b + a$, se cumple la propiedad 1. Si $a + d = b + c$, entonces $c + b = d + a$ y se cumple la propiedad 2. En la propiedad 3 se desea probar que $a + f = b + e$, dado que $a + d = b + c$ y $c + f = d + e$. Ahora, $(a + d) + f = (b + c) + f = b + (c + f) = b + (d + e)$. Por lo tanto, $(a + f) + d = (b + e) + d$ y de aquí, de acuerdo con la ley de cancelación para los enteros positivos, $a + f = b + e$.

Cualquier relación entre pares de elementos, tales como la igualdad anterior de parejas de enteros positivos, es decir, reflexiva, simétrica y transitiva, recibe el nombre de *relación de equivalencia*. Nótese que esta relación de equivalencia o igualdad, separa el conjunto de pares de enteros positivos en clases de pares mutuamente exclusivas tales que dos miembros cualesquiera de una clase son equivalentes o iguales, mientras que miembros de clases diferentes son no equivalentes o desiguales. Un *entero* se define como una clase de pares equivalentes. Así, por ejemplo, posteriormente se definirá el entero 2 como la clase de todos los pares equivalentes a $(3, 1)$ y el entero -2 como la clase de todos los pares equivalentes a $(1, 3)$. Nótese que, conceptualmente, existe una diferencia entre el entero positivo 2 y el entero 2. Posteriormente, regresaremos a este punto, pero, por el momento, continuaremos con el tratamiento formal de los enteros como clases de pares de enteros positivos.

Definición de adición y multiplicación

Se define* la suma

$$(a, b) + (c, d) = (a + c, b + d)$$

y el producto

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc).$$

Estas definiciones de suma y producto de dos parejas (a, b) y (c, d) realmente son definiciones de suma y producto de la clase de pares que contiene a (a, b) y la clase de pares que contiene a (c, d). Porque podemos sustituir cualquier pareja $(a', b') = (a, b)$ y cualquier pareja $(c', d') = (c, d)$ en las definiciones anteriores y obtener una pareja

$$(a' + c', b' + d') = (a + c, b + d)$$

y una pareja producto

$$(a'c' + b'd', a'd' + b'c') = (ac + bd, ad + bc).$$

Por ejemplo, si $(a', b') = (a, b)$ y $(c', d') = (c, d)$, se tiene $a' + b = b' + a, c' + d = d' + c$ y de aquí

$$(a' + c') + (b + d) = (b' + d') + (a + c).$$

En consecuencia,

$$(a', b') + (c', d') = (a' + c', b' + d') = (a + c, b + d).$$

Mediante una manipulación un poco más complicada, también puede probarse que $(a', b') \cdot (c', d') = (a, b) \cdot (c, d)$. Por lo tanto, las definiciones de suma y producto de dos parejas (a, b) y (c, d), determinan dos clases de parejas, las clases suma y producto, las cuales están determinadas por las clases que contienen (a, b) y (c, d). Por lo tanto, se ha definido la suma y el producto de dos enteros.

Se demuestra fácilmente que la adición y la multiplicación de enteros obedecen las leyes conmutativa, asociativa y distributiva. Por ejemplo, la ley distributiva puede probarse de la manera siguiente:

$$\begin{aligned}
(a, b) \cdot [(c, d) + (e, f)] &= (a, b) \cdot (c + e, d + f) \\
&= (a[c + e] + b[d + f], a[d + f] + b[c + e]) \\
&= ([ac + bd] + [ae + bf], [ad + bc] + [af + be]) \\
&= (ac + bd, ad + bc) + (ae + bf, af + be) \\
&= (a, b) \cdot (c, d) + (a, b) \cdot (e, f).
\end{aligned}$$

* Por supuesto que nuestra motivación para estas definiciones descansa en las identidades del álgebra elemental: $(a - b) + (c - d) = (a + c) - (b + d)$ y $(a - b)(c - d) = (ac + bd) - (ad + bc)$.

Nótese que en la demostración anterior no solamente se aplicaron las definiciones de las nuevas adición y multiplicación, sino también las propiedades asociativa, conmutativa y distributiva de los enteros positivos. Las demostraciones de las otras leyes se dejan al estudiante.

Ejercicios

1. Probar que la adición de los enteros es conmutativa.
2. Probar que la multiplicación de los enteros es conmutativa.
3. Probar que la adición de los enteros es asociativa.
4. Probar que la multiplicación de los enteros es asociativa.

6 · NUMERO CERO

Ahora vamos a investigar más detenidamente las parejas (a, b) respecto de la relación de orden entre los enteros positivos a y b. Recordemos que $a = b$, o $a > b$, o $a < b$. Por tanto, cualquier pareja (a, b) puede escribirse como (a, a), o $(x + b, b)$, o $(a, x + a)$.

Primero se considerarán las propiedades de las parejas (a, a). Se observa que $(a, a) = (b, b)$. Además, si $(a, a) = (b, c)$, entonces $b = c$ porque, de acuerdo con la definición de igualdad, $a + c = a + b$. Así, aquellas parejas en las cuales ambos enteros positivos son iguales, determinan una clase que puede representarse por la pareja (a, a) pero que es independiente del entero a particular. Esta clase recibe el nombre de entero cero y se representará por cualquier pareja en la que ambos enteros positivos son iguales.

Propiedades del cero

Para toda pareja (x, y),

$$(x, y) + (a, a) = (x, y)$$

y

$$(x, y) \cdot (a, a) = (a, a).$$

Estas dos propiedades se deducen inmediatamente a partir de las definiciones, porque

$$(x, y) + (a, a) = (x + a, y + a) = (x, y)$$

y

$$(x, y) \cdot (a, a) = (ax + ay, ax + ay) = (a, a).$$

La primera propiedad mencionada se caracteriza frecuentemente diciendo que el cero es una *identidad para la adición.*

7 · ENTEROS POSITIVOS COMO SUBCONJUNTO DE LOS ENTEROS

Ahora necesitamos definir una *correspondencia biunívoca* entre dos conjuntos de símbolos. Se dice que existe una correspondencia biunívoca entre los elementos de un conjunto A y los elementos de un conjunto B si los elementos de los dos conjuntos pueden parearse de modo que a cada elemento de A le corresponda un y solamente un elemento del conjunto B y si cada elemento de B es el correspondiente o imagen de un y solamente un elemento de A. Por ejemplo, existe una correspondencia biunívoca entre el conjunto de sillas de un salón de clase y el conjunto de estudiantes, si existe una silla para cada estudiante y si existe un estudiante para cada silla.

Consideremos ahora las parejas $(x + b, b)$. Se observa que $(x + b, b) = (x + c, c)$. Además, $(x + b, b) = (y + c, c)$ solamente si $x = y$. De aquí que todas las parejas $(x + b, b)$ representan solamente un entero determinado, donde x es fijo y b es cualquier entero positivo. Por lo tanto, podemos establecer una correspondencia biunívoca entre las clases representadas por las parejas $(x, + b, b)$ y los enteros positivos, de la manera siguiente. Denotaremos la correspondencia escribiendo

$$(x + b, b) \leftrightarrow x.$$

Por lo tanto, a cada clase representada por $(x + b, b)$, donde x es fijo, le asignamos el entero positivo x, y a cada entero positivo x le asignamos la clase representada por $(x + b, b)$. Ahora, si

$$(x + b, b) \leftrightarrow x \qquad \text{y} \qquad (y + c, c) \leftrightarrow y,$$

entonces

$$(x + b, b) + (y + c, c) = (x + y + b + c, b + c) \leftrightarrow x + y^*$$

y

$$(x + b, b) \cdot (y + c, c) =$$
$$(xy + xc + by + bc + bc, xc + by + bc + bc) \leftrightarrow xy.$$

Una correspondencia biunívoca de este tipo en la cual se conservan la adición y la multiplicación se llama *isomorfismo*. Así, se ve que las clases de parejas (a, b) para las cuales $a > b$, pueden considerarse simplemente

* Para ahorrar espacio ya no indicaremos por medio de paréntesis el uso de la ley asociativa para la adición para los enteros positivos. Ahora está claro el significado de $a + b + c$.

como símbolos diferentes para los enteros positivos ya que tienen las mismas propiedades que los enteros positivos. Por ejemplo, entonces, el entero positivo 2 corresponde a la clase de todas las parejas equivalentes a $(2 + 1, 1) = (3, 1)$. Ahora se verá que, aunque el entero positivo 2 no es idéntico al entero 2, se tiene entero positivo 2 $\leftrightarrow$ entero 2.

Resumiendo, se ha demostrado el teorema siguiente:

Teorema 2. Las clases de parejas (a, b), *con* $a > b$, *son isomorfas para los enteros positivos.*

Ejercicios

1. Sea A el conjunto de los enteros positivos y B el conjunto de los enteros positivos pares. ¿La correspondencia $n \leftrightarrow 2n$, cuando n es un entero positivo, es una correspondencia biunívoca? ¿Se conserva bajo la adición? ¿Bajo la multiplicación?
2. Sea A el conjunto de los enteros y B el conjunto de los enteros positivos. ¿La correspondencia $n \leftrightarrow n^2$, cuando n es un entero, es una correspondencia biunívoca? ¿Se conserva bajo la adición? ¿Bajo la multiplicación?
3. Probar que la clase de parejas (a, b) con $a \geq b$ no es isomorfa para los enteros positivos.

8 · ENTEROS NEGATIVOS

Hasta el momento, por medio de nuestros nuevos símbolos (a, b) sólo se ha presentado esencialmente un nuevo número, a saber, el cero. Entonces, el tercer tipo de parejas (a, b), con $a < b$, representan números diferentes al cero y a los enteros positivos. Estos números pueden escribirse en la forma $(a, x + a)$, y como en el caso de las parejas $(x + b, b)$, por medio de las parejas $(a, x + a)$, donde x es fijo y a es cualquier otro entero positivo, solamente se representa una clase determinada o entero. A estas clases de parejas se les dará el nombre de *enteros negativos*. Por ejemplo, -2 puede definirse como la clase de todas las parejas equivalentes a $(1, 2 + 1) = (1, 3)$.

Así, se ha extendido nuestro sistema de numeración. Puesto que un subconjunto de las clases de parejas de enteros positivos puede identificarse con los enteros positivos, se dice que los enteros positivos han quedado *incluidos* en el sistema de enteros. Además, ahora puede encontrarse una solución x en el sistema de enteros para la ecuación $a + x = b$, donde a y b denotan enteros. Primero se demostrarán las siguientes leyes de cancelación.

Teorema 3. Si $(a,b) + (c,d) = (a,b) + (e,f)$, *entonces* $(c,d) = (e,f)$. *Si* $(x,y) \cdot (a,b) = (x,y) \cdot (c,d)$ *y* $(x,y) \neq (z,z)$, *entonces* $(a,b) = (c,d)$.

La ley de cancelación para la adición se demuestra fácilmente aplicando la ley de cancelación para los enteros positivos. Se tiene $(a+c, b+d) = (a+e, b+f)$. De aquí que $a+c+b+f = b+d+a+e$. Por lo tanto, $(c+f)+(a+b) = (d+e)+(a+b)$, $c+f = d+e$ y se tiene $(c,d) = (e,f)$.

Para probar la ley de cancelación para la multiplicación, primero supóngase que (x,y) representa un entero negativo y sea $y = x+z$. Entonces $(x, x+z) \cdot (a,b) = (x, x+z) \cdot (c,d)$. Efectuando la multiplicación y aplicando la definición de igualdad y, finalmente, las leyes de cancelación para los enteros positivos, se tiene el resultado deseado $b+c = a+d$. La demostración cuando (x,y) representa un entero positivo es semejante.

Teorema 4. La ecuación $(a,b) + (x,y) = (c,d)$ *tiene una solución única.*

Nótese que $(a,b) + (c+b, d+a) = (a+c+b, b+d+a) = (c,d)$. De aquí que $(c+b, d+a)$ es una solución. Ahora, sea (u,v) una solución cualquiera. Entonces, $(a,b) + (c+b, d+a) = (a,b) + (u,v)$ y, de acuerdo con la ley de cancelación para la adición, se tiene $(u,v) = (c+b, d+a)$.

La solución $(x,y) = (c+b, d+a)$ se conoce como la *diferencia*, $(c,d) - (a,b)$, y la operación de encontrar esta diferencia se llama *sustracción*. En particular, la solución (x,y), de la ecuación $(a,b) + (x,y) = (z,z)$, es $(z,z) - (a,b) = (z+b, z+a) = (b,a)$. Este número se denotará por $-(a,b)$ y $-(a,b)$ se conoce como el *inverso aditivo* de (a,b).

Ahora que se han establecido las propiedades básicas de los enteros, ya no es necesario utilizar la notación de parejas de enteros positivos. Se escribe 0 para la clase de parejas equivalentes a $(1,1)$, $+1$ para la clase de parejas equivalentes a $(2,1)$, -1 para la clase de parejas equivalentes a $(1,2)$, etc. Como una simplificación adicional se escribe 1 por $+1$, 2 por $+2$, etc., y, si se denota un entero cualquiera por y, su inverso aditivo se denota por $-y$. Así, si $y = +2$, $-y = -2$, mientras que si $y = -2$, $-y = +2$.

Hemos visto que las operaciones de adición y multiplicación de los enteros son conmutativas y asociativas, y que la multiplicación es distributiva respecto de la adición. La ley de cancelación para la adición se

cumple en la misma forma que para los enteros positivos. La ley de cancelación para la multiplicación se cumple con una ligera modificación: si a, b y x son enteros, $ax = bx$ implica $a = b$ solamente si $x \neq 0$.

Ahora pueden probarse muchas de las propiedades conocidas de los enteros, aplicando las propiedades representativas de las clases que definen los enteros. Por ejemplo, para probar que, si y es un entero cualquiera, $-(-y) = y$, se considera que (a,b) representa a y. Entonces, $-(a,b) = (b,a)$ representa $-y$ y $-(b,a) = (a,b)$ representa $-(-y)$. De aquí que $-(-y) = y$.

Ejercicios

1. Completar la demostración del teorema 3.
2. Probar las afirmaciones siguientes para los enteros x, y y z:
   a. $(-x)(-y) = xy$.
   b. $(-x)y = x(-y) = -(xy)$.
   c. $-(x+y) = (-x) + (-y)$.
   d. $-(x-y) = (-x) + y$.
   e. $x(y-z) = xy - xz$.
   f. $(x-y) + (y-z) = x - z$.
3. Probar que los enteros negativos no son isomorfos para los enteros positivos.
4. Probar: Si x y y son enteros y $xy = 0$, entonces $x = 0$ o bien $y = 0$.
5. Probar por inducción para los enteros positivos n:
   a. $1 + 3 + \cdots + (2n-1) = n^2$.
   b. $1 + 5 + \cdots + (4n-3) = n(2n-1)$.
   c. $1^3 + 3^3 + \cdots + (2n-1)^3 = n^2(2n^2-1)$.
   d. $2 + 2^2 + 2^3 + \cdots + 2^n = 2(2^n - 1)$.
   e. $1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n = (n-1)2^{n+1} + 2$.

9 · DESIGUALDADES

A continuación se definirán las desigualdades entre los enteros en términos de los enteros positivos. Se dice que el entero a es *menor que* el entero b o que el entero b es *mayor que* el entero a si y solamente si $b - a$ es un entero positivo. Se escribe $a < b$ o $b > a$. Así, por ejemplo, $-5 < -3$ y $-3 > -5$ puesto que $-3 - (-5) = 2$ es un entero positivo. Partiendo de la definición pueden demostrarse las siguientes propiedades de los enteros:

1. Si $a < b$ y $b < c$, entonces $a < c$.
2. Si $a < b$, entonces $a + c < b + c$.
3. Si $a < b$ y $c > 0$, entonces $ac < bc$.
4. Si $a < b$ y $c < 0$, entonces $ac > bc$.

Por ejemplo, si $a < b$ y $b < c$, entonces $b - a$ y $c - b$ son enteros positivos. De aquí que $(b-a) + (c-b) = c - a$ es un entero positivo y se concluye que $a < c$.

Valor absoluto

Para un entero dado a se tiene $a = 0$, o $a > 0$, o $-a > 0$. Así, se define el valor absoluto de a: $|a| = 0$, o a, o $-a$, de acuerdo con que se tenga $a = 0$, $a > 0$ o $-a > 0$. Las dos propiedades del valor absoluto que se necesitarán son

$$|a| \cdot |b| = |ab| \qquad \text{y} \qquad |a + b| \leq |a| + |b|,$$

y pueden demostrarse fácilmente mediante una consideración sobre las diversas posibilidades para a y b como enteros positivos o negativos o cero. Como un ejemplo, se probará la segunda desigualdad. Si tanto a como b son positivos o ambos negativos, o si por lo menos uno es cero, fácilmente se ve que se cumple el signo de desigualdad. Si a es positivo y b es negativo se tiene $|a| = a$ y $|b| = -b$. Entonces, si $a + b$ es negativo, $|a + b| = -(a + b)$. Pero, puesto que a es positivo, $-(a + b) = -a - b < a - b = |a| + |b|$. Si $a + b$ es no negativo, $|a + b| = a + b$ y $a + b < a - b$. Si a es negativo y b es positivo simplemente se intercambian los papeles de a y b.

Ejercicios

1. Probar que, si a, b y c son enteros, entonces:
   a. Si $a < b$, entonces $a + c < b + c$.
   b. Si $a < b$ y $c > 0$, entonces $ac < bc$.
   c. Si $a < b$ y $c < 0$, entonces $ac > bc$.
2. Probar que $|a| \cdot |b| = |ab|$ para todos los enteros a y b.
3. Si x y y son enteros tales que $xy = 1$, probar que $x = y = 1$ o $x = y = -1$.
4. Probar por inducción que para todos los enteros positivos $n > 1$, $n^3 + 1 > n^2 + n$.
5. Probar por inducción que para todos los enteros positivos n, $2^n > n$.

10 · DIVISION DE ENTEROS

Hemos visto que el conjunto de los enteros es cerrado respecto de la adición, la sustracción y la multiplicación. Sin embargo, el conjunto de los enteros no es cerrado respecto de la división, definida de la manera siguiente:

Definición de división

Se dice que un entero a es divisible por un entero b si existe un entero c tal que $a = bc$. Se escribe $b \mid a$ y se dice que b es un *divisor* de a y que a es un *múltiplo* de b.

Se observa que la relación de divisibilidad es reflexiva y transitiva. Porque $a \mid a$ y, además, si $a \mid b$ y $b \mid c$, entonces existen los enteros x y y tales que $ax = b$ y $by = c$, de modo que $(ax)y = a(xy) = by = c$ y $a \mid c$.

Asociados

Dos enteros a y b diferentes de cero se llaman asociados si tanto $a \mid b$ como $b \mid a$. Puesto que $a = bc$ y $b = ad$, $a = adc$. Aplicando la ley de cancelación para la multiplicación $dc = 1$ y de aquí que $d = 1$ o -1 y $c = 1$ o -1. Por lo tanto, los únicos asociados de a son a y $-a$.

Unidades

Un asociado del entero 1 se llama unidad. De aquí que las únicas unidades son 1 y -1.

Primos

Un entero p diferente de cero es un primo si no es 1 ni -1 y si solamente sus divisores son 1, -1, p y $-p$.

Ejercicios

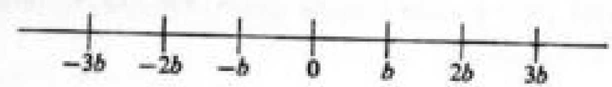
1. Encontrar los divisores de 24.
2. Hacer una lista de los primeros 15 primos positivos.
3. Encontrar los divisores primos positivos de 112.
4. Probar: Si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$.
5. Si $b \mid a$ y $a \neq 0$, entonces $|b| \leq |a|$.
6. Si $b \mid a$ y $|a| < |b|$, entonces $a = 0$.
7. Probar por inducción las siguientes proposiciones para todos los enteros positivos n:
   a. $8^n - 3^n$ es divisible entre 5.
   b. $3^{2n+2} - 8n - 9$ es divisible entre 64.
   c. $9^n - 8n - 1$ es divisible entre 64.
   d. $7^{2n} - 48n - 1$ es divisible entre 2304.

11 · MAXIMO COMUN DIVISOR

Teorema 5. El algoritmo de la división. Dados dos enteros a *y* b *con* $b > 0$, *existe un par único de enteros* q *y* r *tales que* $a = bq + r$, *donde* $0 \leq r < b$.

Para motivar la demostración consideremos a los enteros distribuidos sobre una recta donde todos los múltiplos posibles, bq, de b, forman

un conjunto de puntos igualmente espaciados sobre la recta, como se muestra a continuación:



Es evidente que el punto que representa a a debe encontrarse en uno de los intervalos determinados por estos puntos. Supóngase que se encuentra en el intervalo entre bq y $b(q+1)$ (excluyendo el punto de la derecha). Entonces $a - bq = r$, donde r representa una longitud más corta que toda la longitud del intervalo y, por lo tanto, $0 \leq r < b$, tal y como se afirmó.

Ahora procederemos a desarrollar una demostración algebraica basada en este punto de vista geométrico. Por tanto, consideremos el conjunto de enteros $a - bx$. Este conjunto contiene, por lo menos, un entero no negativo, a saber $a - (-|a|)b$. Porque si $b > 0$, $b \geq 1$ y $-|a|b \leq -|a| \leq a$. Por lo tanto, el conjunto contiene a cero o a un entero positivo lo menor posible. Sea este entero no negativo $r = a - bq$. Ahora, $r \geq 0$ y, si $r \geq b$, entonces $0 \leq r - b = a - bq - b = a - (q+1)b < r$, conclusión contraria a la forma en que se escogió r. Por lo tanto, se ha establecido la existencia de los enteros r y q deseados. El entero r recibe el nombre de *residuo* y el entero q el de *cociente*. Para probar la unicidad de q y r, supóngase que existe un segundo par de enteros q' y r' tales que $a = bq' + r'$, donde $0 \leq r' < b$. Entonces $bq' + r' = bq + r$ y $r' - r = (q - q')b$ lo que implica que b divide a $r' - r$. Pero $|r' - r| < b$. De aquí que $r' - r = 0$ y, puesto que $b \neq 0$, $q' - q = 0$.

Máximo común divisor

Un entero d es el máximo común divisor de dos enteros a y b si $d \mid a$ y $d \mid b$ y, si c es cualquier divisor común de a y b, $c \mid d$. Es fácil ver que, si a, o b, es cero, entonces el entero diferente de cero es un máximo común divisor. Si tanto a como b son cero, definiremos el cero como el máximo común divisor. Además, obsérvese que, de acuerdo con la definición, dos máximos comunes divisores cualesquiera de dos enteros diferentes de cero deben ser asociados. De aquí que, si dos enteros diferentes de cero, a y b, tienen un máximo común divisor, entonces tienen un máximo común divisor positivo que denotaremos por (a, b) y llamaremos el *m.c.d.*; por ejemplo, $(9, 12) = 3$.

Teorema 6. El algoritmo euclidiano. Dos enteros cualesquiera, diferentes de cero, a y b, *tienen un máximo común divisor positivo.*

La demostración también nos proporcionará un método para encontrar el máximo común divisor. Puesto que dos máximos común divisores cualesquiera de a y b son asociados, puede suponerse que tanto a como b son positivos. Escribiremos $a = bq + r$, $0 \leq r < b$. Si $r = 0$, entonces b es el m.c.d. de a y b. Si $r \neq 0$, se demostrará que $(a, b) = (b, r)$. Sea $d = (a, b)$ y $d' = (b, r)$. Ahora, d divide a a y b, y de aquí que d divide a $a - bq = r$ y es un divisor común de b y r. Por tanto, $d \mid d'$. En forma semejante, d' divide a b y r y, por lo tanto, d' divide a $bq + r = a$ y es un divisor común de a y b. De aquí que $d' \mid d$. Por lo tanto, $d = d'$ y el problema de encontrar el máximo común divisor de a y b se ha reducido al de encontrar el máximo común divisor de b y r.

Ahora, al aplicar el algoritmo de la división a b y r, obtenemos $b = rq_1 + r_1$, $0 \leq r_1 < r$. Si $r_1 = 0$, r es el m.c.d. de b y r. Si $r_1 \neq 0$, $(b, r) = (r, r_1)$, y el problema de encontrar el m.c.d. de b y r se ha reducido al de encontrar el m.c.d. de r y r_1. Continuando en esta forma se obtienen las siguientes igualdades:

$$\begin{array}{ll}
a = bq + r, & 0 < r < b, \\
b = rq_1 + r_1, & 0 < r_1 < r, \\
r = r_1q_2 + r_2, & 0 < r_2 < r_1, \\
r_1 = r_2q_3 + r_3, & 0 < r_3 < r_2, \\
\cdots & \cdots \\
r_j = r_{j+1}q_{j+2} + r_{j+2}, & 0 < r_{j+2} < r_{j+1}.
\end{array}$$

Ya que los r_j forman un conjunto decreciente de enteros no negativos, debe existir un r_{n+1} igual a cero. De aquí que

$$\begin{array}{ll}
r_{n-2} = r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1}, \\
r_{n-1} = r_nq_{n+1}. &
\end{array}$$

Ahora, $(a, b) = (b, r) = (r, r_1) = \cdots = (r_{n-1}, r_n) = r_n$. Por lo tanto, el máximo común divisor de a y b es r_n.

Teorema 7. Si d = (a, b), *existen los enteros* m *y* n *tales que* d = ma + nb.

Este teorema puede probarse expresando los residuos sucesivos r_j, obtenidos mediante el algoritmo euclidiano, en términos de a y b, tal y como se indica a continuación:

$$r = a - bq = a + (-q)b,$$
$$r_1 = b - rq_1 = b - (a - bq)q_1 = (-q_1)a + (1 + qq_1)b, \text{ etc.}$$

Puede realizarse una demostración general por inducción. Se denota r por r_0 y q por q_0. Ahora se supone que $r_j = m_j a + n_j b$, donde m_j y n_j son enteros, para todos los enteros no negativos $j < k$. Se ha comprobando que esta ecuación se cumple para $j = 0$ y $j = 1$. Entonces, se tiene

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1}q_k \text{ (de acuerdo con el algoritmo euclidiano)} \\ &= m_{k-2}a + n_{k-2}b - (m_{k-1}a + n_{k-1}b)q_k \text{ (de acuerdo con nuestra hipótesis de inducción)} \\ &= (m_{k-2} - m_{k-1}q_k)a + (n_{k-2} - n_{k-1}q_k)b, \end{aligned}$$

y se completa la demostración. Por lo tanto, r_n puede expresarse como una función lineal de a y b con coeficientes enteros.

EJEMPLO: Encontrar el m.c.d. de 595 y 252 y expresarlo en la forma $252m + 595n$. Se tiene

$$\begin{aligned} 595 &= 2 \cdot 252 + 91, \\ 252 &= 2 \cdot 91 + 70, \\ 91 &= 1 \cdot 70 + 21, \\ 70 &= 3 \cdot 21 + 7, \\ 21 &= 3 \cdot 7. \end{aligned}$$

De aquí que $(252, 595) = 7$. Para encontrar m y n es conveniente empezar con el último residuo diferente de cero. Por lo tanto (subrayando los residuos y 252 y 595, para no perderlos de vista):

$$\begin{aligned} 7 &= \underline{70} - 3 \cdot \underline{21} \\ &= \underline{70} - 3(\underline{91} - 1 \cdot \underline{70}) = 4 \cdot \underline{70} - 3 \cdot \underline{91} \\ &= 4(\underline{252} - 2 \cdot \underline{91}) - 3 \cdot \underline{91} = -11 \cdot \underline{91} + 4 \cdot \underline{252} \\ &= -11(\underline{595} - 2 \cdot \underline{252}) + 4 \cdot \underline{252} = 26 \cdot \underline{252} + (-11)\underline{595}. \end{aligned}$$

Obsérvese que m y n no son únicos. Por ejemplo,

$$7 = (26 + 595)252 - (11 + 252)595 = 621 \cdot 252 + (-263)595.$$

Ejercicios

1. Encontrar $(294, 273)$ y expresarlo en la forma $294m + 273n$ de dos maneras.
2. Encontrar $(163, 34)$ y expresarlo en la forma $163m + 34n$ de dos maneras.
3. Encontrar $(6432, 132)$ y expresarlo en la forma $132m + 6432n$.
4. Encontrar $(3456, 7234)$.
5. Probar que si $m > 0$, $(ma, mb) = m(a, b)$.
6. Probar que $[(a, b), c] = [a, (b, c)] = [(a, c), b]$.
7. Probar que si $(a, m) = (b, m) = 1$, entonces $(ab, m) = 1$.
8. Probar que si $(a, c) = d$, $a \mid b$ y $c \mid b$, entonces $ac \mid bd$.

12 · FACTORES PRIMOS

Teorema 8. Si p *es un primo y si* $p \mid ab$, a *y* b *enteros, entonces* $p \mid a$ *o* $p \mid b$.

Puesto que p es primo, sus únicos divisores son ± 1 y $\pm p$. Por lo tanto, si p no divide a a, el m.c.d. de a y p es 1. De acuerdo con el teorema anterior, existen los enteros m y n tales que $1 = ma + np$. Ahora, $b = mab + npb$. Puesto que p es un factor del segundo miembro de esta ecuación, por definición, divide a b y queda demostrado el teorema.

Corolario. Si p *es primo y divide al producto de los enteros* $a_1a_2 \cdots a_n$, *entonces* p *divide a uno de los enteros* a_i.

Aplicando repetidas veces el teorema precedente, se llega inmediatamente a este resultado.

DEFINICIÓN. Si $(a, b) = 1$, se dice que los dos enteros a y b son *primos relativamente*.

Teorema 9. Si $(a, b) = 1$ *y si* $b \mid ac$, *entonces* $b \mid c$.

La demostración es semejante a la demostración del teorema precedente, ya que por hipótesis existen los enteros m y n tales que $1 = ma + nb$, se concluye que $c = mac + nbc$.

Teorema 10. Teorema de la factorización única para los enteros. Todo entero a, $|a| > 1$, *puede expresarse como una unidad multiplicada por un producto de primos positivos. Esta representación es única excepto por el orden en que se presentan los factores primos.*

Sea a el entero que se factoriza. Si a es primo, el entero ha sido representado de acuerdo con el teorema. Por lo tanto, sea a un entero *compuesto*, es decir, ni unidad, ni primo. Ahora, supóngase que el teorema es verdadero para todos los enteros menores que $|a|$. Puesto que a es compuesto, $|a| = |b| \cdot |c|$, donde $|b|$ y $|c|$ son enteros menores que $|a|$. De aquí que, aplicando la hipótesis de la inducción, $|b| = p_1p_2 \cdots p_s$ y $|c| = q_1q_2 \cdots q_t$, donde p_i y q_j son primos positivos. Así

$$|a| = |b| \cdot |c| = p_1p_2 \cdots p_sq_1q_2 \cdots q_t,$$

y queda por demostrar que la representación es única excepto por el orden en que se presentan los factores primos. Supóngase que existiera

una segunda factorización $a = p_1'p_2' \cdots p_v'$. Entonces $p_1'p_2' \cdots p_v' = p_1p_2 \cdots p_sq_1q_2 \cdots q_t$. Ahora, de acuerdo con el corolario anterior, p_1' divide a uno de estos primos, digamos p_1; y de aquí que $p_1' = p_1$. Por lo tanto,

$$p_2'p_3' \cdots p_v' = p_2 \cdots p_sq_1 \cdots q_t.$$

Aplicando el mismo razonamiento un número finito de veces, a estos productos iguales, se obtiene $v = s + t$ y, en consecuencia, una factorización única de $|a|$ y, por lo tanto, de a.

Nótese que el teorema no excluye la presencia de primos iguales. De aquí que el entero puede escribirse

$$a = \pm p_1^{a_1}p_2^{a_2} \cdots p_n^{a_n}, \text{ donde } 1 < p_1 < p_2 < \cdots < p_n,$$

y se ha demostrado que tanto los exponentes a_i como los primos están unívocamente determinados.

Ejercicios

1. Ilustrar el teorema de la factorización única para los enteros 576, -321 y 5244.
2. ¿Qué puede concluirse acerca del m.c.d. de a y b si existen los enteros x y y tales que $ax + by = 1$? ¿Si $ax + by = 3$?
3. Si $d = (a, b)$, $a = a_1d$, $b = b_1d$, entonces $(a_1, b_1) = 1$.
4. Si $(a, b) = 1$ y $a \mid c$ y $b \mid c$, entonces $ab \mid c$.
5. Probar que $2m^2 = n^2$ es una ecuación imposible en los enteros cuando $(m, n) = 1$.
6. Si $(a, b) = 1$, entonces $(a + b, a - b) = 2$ ó 1.
7. Si $(c, d) = 1$, entonces $(c^n, d) = 1$, donde n es un entero positivo.
8. Probar que el número de primos es infinito. *Sugerencia:* Suponer que el número de primos es finito y formar su producto $p_1p_2 \cdots p_n$. Entonces considerar el entero $p_1p_2 \cdots p_n + 1$.
9. Demostrar que $2^{2n} + 1$ es divisible entre 5 cuando n es un entero positivo impar.
10. Demostrar que $2^{2n} - 1$ es divisible entre 5 cuando n es un entero positivo par.

13 · CONGRUENCIAS

DEFINICIÓN. Se dice que dos enteros a y b son *congruentes módulo en un entero positivo* m si y solamente si existe un entero k tal que $a - b = km$. Nótese que esta definición afirma simplemente que m divide a $a - b$. Se escribe $a \equiv b \pmod{m}$ y m recibe el nombre de *módulo* de la congruencia. Por ejemplo, $7 \equiv 15 \pmod 4$, porque $7 - 15 = 4(-2)$.

Teorema 11. La relación, congruencia módulo m, *es:*

1. *Reflexiva:* $a \equiv a \pmod{m}$.
2. *Simétrica: si* $a \equiv b \pmod{m}$, *entonces* $b \equiv a \pmod{m}$.
3. *Transitiva: si* $a \equiv b \pmod{m}$ *y* $b \equiv c \pmod{m}$, *entonces* $a \equiv c \pmod{m}$.

Estas propiedades se deducen inmediatamente a partir de la definición de congruencia. Por ejemplo, la propiedad transitiva puede demostrarse de la manera siguiente: Puesto que $a - b = km$ y $b - c = nm$, se obtiene $a - c = (k + n)m$ al sumar, y éste es el resultado deseado.

Es de esperarse, con base en este teorema que, en muchos aspectos, las congruencias se comportan como igualdades. Esta semejanza queda ilustrada en los tres teoremas siguientes.

Teorema 12. Si $a \equiv b \pmod{m}$, *entonces* $a + x \equiv b + x$ *y* $ax \equiv bx \pmod{m}$ *para todos los enteros* x.

Como en el teorema anterior, la demostración es inmediata a partir de la definición y, en consecuencia, se deja al estudiante.

Teorema 13. Si $a \equiv b$ *y* $c \equiv d \pmod{m}$, *entonces* $a + c \equiv b + d$, $a - c \equiv b - d$ *y* $ac \equiv bd \pmod{m}$.

Cada una de estas afirmaciones puede demostrarse directamente a partir de la definición. Sin embargo, la última se demuestra en forma más sencilla aplicando la segunda parte del teorema 12 y la propiedad transitiva de las congruencias, de la manera siguiente: $ac \equiv bc$ y $bc \equiv bd \pmod{m}$ y, por lo tanto, $ac \equiv bd \pmod{m}$.

Teorema 14. Si $ca \equiv cb \pmod{m}$ *y* $d = (c, m)$, *de modo que* $m = dw$, *entonces* $a \equiv b \pmod{w}$.

Ahora, $c = dv$ y $m = dw$, donde $(v, w) = 1$. Además, $dw \mid c(a - b)$ y de aquí que $w \mid v(a - b)$. Así, puesto que $(v, w) = 1$, $w \mid (a - b)$. Si $d = 1$, se obtiene el siguiente teorema:

Teorema 15. Si $ca \equiv cb \pmod{m}$ *y* $(c, m) = 1$, *entonces* $a \equiv b$ (*mod.* m).

Una definición alternativa de la congruencia, de gran utilidad, se incorpora en el teorema siguiente.

Teorema 16. $a \equiv b \pmod{m}$ *si y solamente si* a *y* b *dejan el mismo residuo cuando se dividen entre* m.

Si $a \equiv b \pmod{m}$, entonces $b - a = km$. Sea $a = mq + r$, $0 \leq r < m$. Ahora, $b = a + km = mq + r + km = (q + k)m + r$ con lo que se establece que r es el residuo cuando se divide b entre m. Por otra parte, si $a = mq + r$ y $b = mq_1 + r$, $0 \leq r < m$, entonces $a - b = (q - q_1)m$ y $a \equiv b \pmod{m}$.

Por lo tanto, cualquier entero a es congruente módulo m a su residuo r. De aquí que, de acuerdo con la propiedad transitiva de las congruencias, puede sustituirse r por a en cualquier congruencia módulo m. Por ejemplo, si $313x \equiv 7 \pmod{10}$, entonces $3x \equiv 7 \pmod{10}$ es una proposición equivalente, porque $313 \equiv 3 \pmod{10}$ y $313x \equiv 3x \pmod{10}$.

Ejercicios

1. Completar la demostración del teorema 11.
2. Probar el teorema 12.
3. Completar la demostración del teorema 13.
4. Encontrar los enteros positivos menores módulo 7 para los cuales son congruentes los enteros 22, 312 y $22 \cdot 312$.
5. Encontrar el menor entero positivo módulo 11 para el cual es congruente el producto $3 \cdot 7 \cdot 13 \cdot 515 \cdot 23$.
6. Encontrar los enteros positivos menores módulo 5 para los cuales son congruentes las potencias 3^2, 3^3, 3^4, 3^m.
7. Encontrar el menor entero positivo módulo 7 para el cual es congruente 10^{m}.
8. Si $14x \equiv 2 \pmod{8}$, citar los teoremas que nos permiten escribir $7x \equiv 1 \pmod{4}$, $6x \equiv 2 \pmod{8}$ y $3x \equiv 1 \pmod{4}$.
9. Si m es un entero, entonces $m^2 \equiv 0$ ó $1 \pmod{4}$.
10. Confirmar que todo entero positivo puede expresarse de la manera siguiente:

$$a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0,$$

donde a_i son enteros comprendidos entre 0 y 9. De aquí que, si un entero positivo es divisible entre 9, la suma de su dígitos es divisible entre 9.

14 · CONGRUENCIA LINEAL

A continuación se discutirá la congruencia lineal $ax \equiv b \pmod{m}$. Nótese que, si x_1 es una solución, es decir, $ax_1 \equiv b \pmod{m}$, entonces cualquier otro entero $x_2 \equiv x_1 \pmod{m}$ también es una solución ya que se tiene $ax_2 \equiv ax_1 \equiv b \pmod{m}$. Generalmente se toman los enteros en el intervalo $0 \leq x < m$ como representativos de las soluciones.

Teorema 17. La congruencia $ax \equiv b \pmod{m}$ *tiene una solución si y solamente si el máximo común divisor* d *de* a *y* m *divide a* b. *Si* d *divide a* b, *la congruencia tiene exactamente* d *soluciones incongruentes módulo* m.

Considérese que $ax \equiv b \pmod{m}$ tiene una solución x_1. Entonces $ax_1 - b = km$ y $d = (a, m)$ necesariamente divide a b. Ahora, dado que d divide a b, se pretende obtener las soluciones de la congruencia. Puesto que $d = (a, m)$, existen los enteros x_1 y y_1 tales que $ax_1 + my_1 = d$. Ahora, $b = b_1 d$, y multiplicando la expresión lineal para d por b_1, se tiene $a(x_1 b_1) + m(y_1 b_1) = db_1 = b$. Por lo tanto, $x_1 b_1$ es una solución de la congruencia $ax \equiv b \pmod{m}$.

Falta por demostrar que existen d soluciones incongruentes módulo m. Ahora, $m = m_1 d$ y $a = a_1 d$. De aquí que una solución x de la congruencia $ax \equiv b \pmod{m}$ también es una solución de la congruencia $a_1 x \equiv b_1 \pmod{m_1}$ y recíprocamente. Dos soluciones cualesquiera de $a_1 x \equiv b_1 \pmod{m_1}$ son congruentes módulo m_1. Esto es, sean x_0 y x_1 dos soluciones cualesquiera. Entonces $a_1 x_0 \equiv b_1 \equiv a_1 x_1 \pmod{m_1}$ y, puesto que $(a_1, m_1) = 1$, $x_0 \equiv x_1 \pmod{m_1}$. De aquí que todas las soluciones incongruentes módulo m de $ax \equiv b \pmod{m}$, se encuentran entre los enteros $x_0 + km_1$. Se desea demostrar que el conjunto de enteros $x_0 + km_1$ contiene exactamente d enteros incongruentes módulo m, cuyos representantes son $x_0, x_0 + m_1, x_0 + 2m_1, \cdots, x_0 + (d - 1)m_1$. Primero, estos representantes son todos incongruentes módulo m porque, si $x_0 + r_1 m_1 \equiv x_0 + r_2 m_1 \pmod{m}$, donde $r_1 < d$ y $r_2 < d$, entonces $r_1 m_1 \equiv r_2 m_1 \pmod{m}$ y $r_1 \equiv r_2 \pmod{d}$; pero $|r_1 - r_2| < d$ y de aquí que $r_1 = r_2$. Segundo, todo entero $x_0 + km_1$ es congruente a uno de los representantes anteriores porque $k = qd + r$, donde $0 \leq r < d$, y $x_0 + km_1 = x_0 + (qd + r)m_1 \equiv x_0 + rm_1 \pmod{m}$.

Al resolver cualquier congruente lineal, obsérvese primero si puede simplificarse aplicando todas las propiedades de las congruencias que se han desarrollado. Por ejemplo, $x + 50 \equiv 39 \pmod{7}$ es equivalente a $x + 1 \equiv 4 \pmod{7}$ y de aquí que $x \equiv 3 \pmod{7}$. Asimismo, si $235x \equiv 54 \pmod{7}$, entonces $4x \equiv 5 \pmod{7}$ y de aquí $x \equiv 3 \pmod{7}$. En la misma forma, si $29x \equiv 5 \pmod{34}$, entonces $-5x \equiv 5 \pmod{34}$ y $x \equiv -1 \pmod{34}$.

La congruencia $35x \equiv 5 \pmod{14}$ es un ejemplo de una congruencia lineal sin solución, porque $(35, 14) = 7$ y 7 no divide a 5. Por otra parte, $35x \equiv 14 \pmod{21}$ tiene exactamente 7 soluciones incongruentes módulo 21. En este caso se divide entre 7, obteniendo la congruencia $5x \equiv 2 \pmod{3}$ que tiene a 1 como la menor solución positiva. De aquí

que los representantes de las 7 soluciones incongruentes de $35x \equiv 14 \pmod{21}$ en el intervalo $0 \leq x < 21$ son 1, 4, 7, 10, 13, 16 y 19.

Si el módulo es un número grande, el proceso del máximo común divisor nos capacita para encontrar una solución tal y como se ve en la demostración del teorema general. Por ejemplo, en la congruencia $11x \equiv 2 \pmod{317}$, $(317, 11) = 1$ y despejando los residuos en el proceso del máximo común divisor, se encuentra que $1 = 5(317) + 11(-144)$. Entonces, $2 = 10(317) + 11(-288)$ y -288 es una solución. Se toma la solución positiva menor, 29, como una solución representativa.

Ejercicios

Encontrar las soluciones incongruentes de las siguientes congruencias:

1. $x - 3 \equiv 2 \pmod 5$.
2. $2x + 1 \equiv 4 \pmod 5$.
3. $2x + 1 \equiv 4 \pmod{10}$.
4. $3x \equiv 2 \pmod 7$.
5. $51x \equiv 32 \pmod 7$.
6. $13x \equiv 10 \pmod{28}$.
7. $273x \equiv 210 \pmod{588}$.
8. $66x \equiv 8 \pmod{78}$.
9. $104x \equiv 16 \pmod{296}$.
10. $1183x \equiv 481 \pmod{533}$.
11. $572x \equiv 412 \pmod{516}$.
12. $45x \equiv 24 \pmod{348}$.
13. Probar que, si p es un primo y c no congruente a $0 \pmod p$, entonces $cx \equiv b \pmod p$ tiene una solución única módulo p.
14. Encontrar los enteros x y y tales que $313x + 45y = 17$.
15. Probar que, si $(m_1, m_2) = 1$, entonces las congruencias $x \equiv b \pmod{m_1}$ y $x \equiv c \pmod{m_2}$ tienen una solución común x y que cualquier par de soluciones son congruentes módulo m_1m_2.

15 · CLASES DE RESIDUOS

Conviene recordar que toda relación entre pares de elementos que sea reflexiva, simétrica y transitiva, recibe el nombre de relación de equivalencia. Por lo tanto, la congruencia módulo m es una relación de equivalencia entre los pares de enteros. Cualquier relación de equivalencia entre los elementos de un conjunto separa los elementos en dos clases de elementos mutuamente exclusivas, de modo que dos elementos cualesquiera de una clase son equivalentes y elementos de clases diferentes no son equivalentes. Así, se separan los enteros en clases módulo m, poniendo en la misma clase a todos aquellos enteros que son congruentes módulo m. Se obtienen clases m porque todo entero es congruente módulo m a su residuo y existen m residuos $0, 1, 2, \cdots, m - 1$. Estas clases, llamadas *clases de residuos módulo m*, son los m conjuntos de enteros km, $km + 1, km + 2, \cdots, km + m - 1$, donde k toma los valores de todos los enteros. Estas clases se denotan por $C_0, C_1, C_2, \cdots,$

$\cdots, C_{m-1}$, respectivamente. Por ejemplo, si $m = 3$, C_0 es el conjunto de todos los enteros divisibles entre 3; C_1 es el conjunto de todos los enteros que tienen un residuo de 1 cuando se dividen entre 3; y C_2 es el conjunto de todos los enteros que tienen un residuo de 2 cuando se dividen entre 3.

La adición y la multiplicación de estas clases de residuos pueden definirse de la manera siguiente: La suma $C_i + C_j$ es la clase que contiene la suma de un entero de C_i y un entero de C_j. El producto C_iC_j es la clase que contiene el producto de un entero de la clase C_i por un entero de la clase C_j. Así, en el ejemplo anterior, $C_0 + C_0 = C_0$; $C_0 + C_1 = C_1$; $C_0 + C_2 = C_2$; $C_1 + C_1 = C_2$; $C_1 + C_2 = C_0$; $C_2 + C_2 = C_1$; $C_0C_0 = C_0C_2 = C_0$; $C_1C_1 = C_1$; $C_1C_2 = C_2$; y $C_2C_2 = C_1$.

Nótese que estas sumas y productos son únicos porque, si a_i y a_i' son dos enteros cualesquiera de C_i, y si a_j y a_j' son dos enteros cualesquiera de C_j, entonces, puesto que $a_i \equiv a_i'$ y también $a_j \equiv a_j'$, $a_i + a_j \equiv a_i' + a_j'$ y $a_ia_j \equiv a_i'a_j' \pmod m$. A partir de estas definiciones puede probarse fácilmente que la adición y la multiplicación de las clases de residuos obedecen las leyes conmutativa, asociativa y distributiva. Se dejan las demostraciones al estudiante.

Ejercicios

1. Para el módulo 6:
   a. Calcular C_2C_3, $(C_4C_3)C_5$, $C_4(C_3 + C_5)$, $C_4C_3 + C_4C_5$.
   b. Encontrar las soluciones C_x de las ecuaciones $C_3 + C_x = C_2$, $C_4C_x = C_1$, $C_i + C_x = C_j$.
   c. ¿Tiene solución la ecuación $C_2C_x = C_3$?
   d. Si $C_2C_x = C_2C_y$, ¿puede concluirse que $C_x = C_y$?
2. Responder las mismas preguntas para el módulo 7.
3. Encontrar una solución C_x de la ecuación $C_i + C_x = C_j$, para el módulo arbitrario m.
4. ¿La ecuación $C_iC_x = C_j$ tiene siempre una solución C_x para el módulo arbitrario m?
5. Probar que: $C_iC_j = C_0$ implica $C_i = C_0$ ó $C_j = C_0$ si y solamente si el módulo m es primo.
6. Probar que:
   a. La adición de clases de residuos es conmutativa.
   b. La multiplicación de clases de residuos es conmutativa.
   c. La adición de clases de residuos es asociativa.
   d. La multiplicación de clases de residuos es asociativa.
   e. La multiplicación de clases de residuos es distributiva respecto de la adición.

16 · NOTACION POSICIONAL PARA ENTEROS

Una aplicación directa de las propiedades de la congruencia de los enteros es el método usado para representar cualquier entero. Recordemos que todo entero se representa por medio de una sucesión con signo de los diez símbolos $0, 1, 2, 3, \cdots, 9$, (es decir, los residuos módulo 10). Esta representación se obtiene en la forma siguiente. Sea a un entero positivo. Por medio del algoritmo de la división, el entero a puede escribirse en la forma $a = 10q_0 + r_0, 0 \leq r_0 < 10$. Si $q_0 = 0$, r_0 es el símbolo usado para a. Si $q_0 > 0$, se aplica otra vez el algoritmo de la división a q_0, obteniendo $q_0 = 10q_1 + r_1, 0 \leq r_1 < 10$. Si $q_1 = 0, a = 10r_1 + r_0$, y el símbolo para a es r_1r_0. Si $q_1 > 0, q_1 = 10q_2 + r_2, 0 \leq r_2 < 10$. Si $q_2 = 0, a = 10(10r_2 + r_1) + r_0 = 10^2r_2 + 10r_1 + r_0$ y el símbolo para a es $r_2r_1r_0$. Si $q_2 > 0$ se repite el proceso. Puesto que los q_i forman un conjunto decreciente de enteros no negativos, el proceso debe cesar en un número finito de pasos. Por tanto

$$a = 10^n r_n + 10^{n-1} r_{n-1} + \cdots + 10r_1 + r_0,$$

y el símbolo para a es $r_n r_{n-1} \cdots r_1 r_0$. Esta representación es única porque, en cualquier paso, los cocientes y los residuos son únicos. Es obvio que los enteros negativos se representan en la misma forma, pero precedidos por un signo menos.

Es evidente que el proceso anterior no depende del entero 10 en particular, llamado base. Cualquier otro entero positivo m (excepto 1) puede usarse como base, y el entero a puede representarse por una sucesión de los m símbolos que representan los m residuos módulo m. Por ejemplo, podría usarse la base 3 y, entonces, el entero puede representarse por medio de los símbolos 0, 1, 2. Ya que 15 puede escribirse como $1 \cdot 3^2 + 2 \cdot 3 + 0$, su símbolo, escrito con la base 3, es 120. Se cumplen las reglas para la adición y la multiplicación, pero, por supuesto, deben aprenderse nuevas tablas si tienen que realizarse los cálculos con rapidez. Las tablas de adición y multiplicación para la base 3 son:

+	0	1	2
0	0	1	2
1	1	2	10
2	2	10	11

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	11

EJEMPLO. Sean los enteros 120 y 121 escritos con la base 3. Encontrar su suma y su producto.

Suma

$$\begin{array}{rl}
120 = & 1 \cdot 3^2 + 2 \cdot 3 + 0 \\
121 = & 1 \cdot 3^2 + 2 \cdot 3 + 1 \\
\hline
1011 = & 2 \cdot 3^2 + 4 \cdot 3 + 1 = 3 \cdot 3^2 + 1 \cdot 3 + 1 \\
 & = 1 \cdot 3^3 + 0 \cdot 3^2 + 1 \cdot 3 + 1
\end{array}$$

Producto

$$\begin{array}{rll}
120 = & 1 \cdot 3^2 + 2 \cdot 3 + 0 & \\
121 = & 1 \cdot 3^2 + 2 \cdot 3 + 1 & \\
\hline
120 & 1 \cdot 3^2 + 2 \cdot 3 + 0 & = 1 \cdot 3^2 + 2 \cdot 3 + 0 \\
1010 & 2 \cdot 3^3 + 4 \cdot 3^2 + 0 \cdot 3 & = 1 \cdot 3^4 + 0 \cdot 3^3 + 1 \cdot 3^2 + 0 \cdot 3 \\
120 & 1 \cdot 3^4 + 2 \cdot 3^3 + 0 \cdot 3^2 & = 1 \cdot 3^4 + 2 \cdot 3^3 + 0 \cdot 3^2 \\
\hline
22{,}220 = & & 2 \cdot 3^4 + 2 \cdot 3^3 + 2 \cdot 3^2 + 2 \cdot 3 + 0
\end{array}$$

Ejercicios

1. Encontrar el símbolo para 26 usando sucesivamente la base 2, 3, 4, 5, 9 y 12.
2. ¿Qué número se representa por medio del símbolo 333, si se interpreta como un número escrito con la base 4? ¿Con la base 5? ¿Con la base 9?
3. Hacer una tabla de adición y otra de multiplicación para la base 5. Encontrar la suma y el producto de 23 y 34 si estos símbolos representan números escritos con la base 5.
4. Un farmacéutico tiene solamente las cinco pesas de 1, 2, 4, 8 y 16 onzas, respectivamente, y una balanza de 2 platillos (las pesas pueden colocarse en ambos platillos). Demostrar que puede pesar cualquier cantidad hasta 31 onzas.
5. Probar que la suma de los dígitos de cualquier múltiplo de 9 es, a su vez, divisible entre 9.

2 Números racionales, reales y complejos

1 · NUMEROS RACIONALES

En el capítulo anterior se vio que el conjunto de enteros no es cerrado respecto de la división. Ahora se definirán los *números racionales* y la adición y multiplicación de números racionales. Se concluirá que la adición y la multiplicación de los números racionales obedecen las leyes conmutativa, asociativa y distributiva. Sin embargo, en la adición, el conjunto de los números es cerrado respecto de la división. Así como se construyeron los enteros usando pares de enteros positivos, en forma semejante se construirán los números racionales usando pares de enteros. La pareja de enteros se denotará por a/b, con $b \neq 0$.

Definición de igualdad

$a/b = c/d$ si y solamente si $ad = bc$. Nótese que esta igualdad no es una igualdad idéntica sino que es una relación reflexiva y simétrica, lo que es evidente, y fácilmente se demuestra que es transitiva. De aquí que es una relación de equivalencia y las parejas de enteros pueden separarse en clases, poniendo en la misma clase todas aquellas parejas que sean iguales. Un número racional se define como la clase de parejas iguales y se representará por cualquier par de enteros perteneciente a la clase que lo define.

A continuación se examinarán estas clases. Nótese que $ma/mb = a/b$, para todos los enteros m diferentes de cero. Además, si el m.c.d. de a y b es m, de modo que $a = a_1m$ y $b = b_1m$, entonces $a/b = a_1/b_1$. Ahora, si $(a, b) = 1$, la igualdad $a/b = c/d$ nos proporciona $ad = bc$ y de aquí

que $c = ma$ y $d = mb$. Por lo tanto, todos los miembros de la misma clase son de la forma ma/mb, donde m es cualquier entero diferente de cero. En la práctica, si $d = (a, b) > 1$, generalmente se sustituye a/b por su igual a_1/b_1, donde $a = a_1d$ y $b = b_1d$. Por tanto, la clase que contiene a a/b puede representarse por a_1/b_1, donde $(a_1b_1) = 1$.

Definición de adición

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Definición de multiplicación

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Con base en nuestra discusión anterior, se observa que, en realidad, la adición y la multiplicación de parejas definen una adición y una multiplicación de clases de parejas puesto que, si cada pareja se reemplaza por otra pareja igual, se obtiene una pareja que pertenece a la clase de la suma o del producto. De aquí que se ha definido la suma y el producto de números racionales.

Aplicando las definiciones anteriores, se verifica fácilmente que la adición y la multiplicación de números racionales obedecen las leyes conmutativa, asociativa y distributiva. Por ejemplo, la ley distributiva,

$$\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}.$$

Puede verificarse de la manera siguiente:

$$\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b}\left(\frac{cf + de}{df}\right) = \frac{acf + ade}{bdf}$$

y

$$\frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} = \frac{ac}{bd} + \frac{ae}{bf}$$

$$= \frac{acbf + aebd}{b^2df}$$

$$= \frac{acf + aed}{bdf}$$

Identidad para la adición

Ya que $a/b + 0/1 = a/b$ para todo a/b, se dice que $0/1$ es una identidad para la adición.

Inverso aditivo

Puesto que $a/b + (-a)/b = (ab - ab)/b^2 = 0/1$, se dice que $(-a)/b$ es un inverso aditivo de a/b.

Identidad para la multiplicación

Puesto que $(a/b)(c/c) = a/b$, se dice que c/c es una identidad para la multiplicación.

Leyes de cancelación para la adición y la multiplicación

El estudiante puede verificar que se cumplen las leyes de cancelación para la adición y la multiplicación, es decir, (1) si $a/b + c/d = a/b + e/f$, entonces $c/d = e/f$, y (2) si $(a/b)(c/d) = (a/b)(e/f)$, $a/b \neq 0/1$, entonces $c/d = e/f$.

División

Una pareja a/b es divisible entre c/d si existe una pareja x/y tal que $a/b = (x/y)(c/d)$. Se ve fácilmente que esa pareja es $(ad)/(bc)$ a menos que $c = 0$. Si $c = 0$, entonces $a = 0$ y x/y es cualquier pareja. Por lo tanto, cualquier número racional es divisible entre cualquier número racional diferente de cero y el conjunto de los números racionales diferentes de cero es cerrado bajo las llamadas *operaciones racionales:* adición, sustracción, multiplicación y división.

Ejercicios

1. Probar que la adición de los números racionales obedece las leyes conmutativa y asociativa.
2. Probar que la multiplicación de los números racionales obedece las leyes conmutativa y asociativa.
3. Probar la ley de cancelación para la adición de los números racionales.
4. Probar la ley de cancelación para la multiplicación de los números racionales.

2 · ENTEROS COMO SUBCONJUNTO DE NUMEROS RACIONALES

Se demostrará que el subconjunto de clases de pares que consiste de aquellas clases de parejas de la forma $a/1$ es isomorfo a los enteros.

Puede establecerse una correspondencia biunívoca de la manera siguiente: Considérese que la clase representada por $a/1$ corresponde al entero a e inversamente el entero a corresponde a esta clase. Ahora, si

$$\frac{a}{1} \leftrightarrow a \quad \text{y} \quad \frac{b}{1} \leftrightarrow b,$$

entonces

$$\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} \leftrightarrow a+b \quad \text{y} \quad \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1} \leftrightarrow ab.$$

Ya que la adición y la multiplicación se conservan bajo esta correspondencia biunívoca, este subconjunto de clases es isomorfo al conjunto de los enteros. Puesto que, abstractamente, estos dos conjuntos de entidades enteramente diferentes son semejantes, los usaremos como si fueran idénticos y, en la práctica, se sustituirá el símbolo para un número racional de este subconjunto por el símbolo para un entero.

3 · NUMEROS REALES

Es evidente que los números racionales no son suficientes para satisfacer las necesidades ordinarias. Por ejemplo, la hipotenusa x de un triángulo rectángulo cuyos catetos son de longitud unitaria, no puede representarse por medio de un número racional porque su cuadrado es 2. Si existiera un número racional p/q, con $(p, q) = 1$, tal que $p^2/q^2 = 2$, entonces $p^2 = 2q^2$, pero se vio (ejercicio 5, pág. 30) que una ecuación de este tipo no tiene solución en los enteros. Para satisfacer tan obvias necesidades, se construyeron los números reales a partir de los números racionales. No se darán los postulados que conducen hacia los números reales y no se demostrará que los números reales obedecen las mismas leyes del álgebra que obedecen los números racionales. Simplemente se describirá la forma de obtener sucesiones de números racionales que sean aproximaciones a los números reales.

Necesitamos recordar el significado de la notación decimal para los números racionales. El número 3.12, por ejemplo, significa

$$3 + \frac{1}{10} + \frac{2}{10^2}.$$

En general, la sucesión de enteros $b.a_1a_2 \cdots a_n$, donde $a_1a_2 \cdots, a_n$ son residuos módulo 10, significa

$$b + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10_n},$$

mientras que la notación $b.a_1a_2 \cdots a_n \cdots$ significa que el decimal no consiste de una sucesión finita de dígitos. Ahora, cualquier número racional puede convertirse en un decimal. Por ejemplo, $32/5 = 6.4$. De acuerdo con el algoritmo de la división se tiene $32 = 6 \cdot 5 + 2$ y, por tanto, 6 es la parte entera de la representación decimal. Ahora, multiplíquese el residuo por 10 y se tiene $20 = 5 \cdot 4$. Por lo tanto, cuatro es el primero y el último dígito después del punto decimal. En forma semejante se encuentra que $1/7$ puede representarse por medio del decimal *periódico* infinito $0.142857142857 \cdots$.

Para convertir cualquier número racional no entero c/d en un decimal, se procede de la misma manera. Es conveniente suponer que c y d son positivos. Se tiene $c = db + r_0$, donde $0 < r_0 < d$ y b es la parte entera de c/d. Entonces $10r_0 = da_1 + r_1$, donde $0 \leq r_1 < d$. Puesto que $r_0 < d$, $10r_0 = da_1 + r_1 < 10d$, y de aquí que $a_1 < 10$. Así, a_1 es el primer dígito después del punto decimal. Si $r_1 = 0, c/d = b + a_1/10 = b.a_1$; pero si $r_1 \neq 0$, se continúa obteniendo $10r_1 = a_2d + r_2$, donde $0 \leq r_2 < d$. Así, $c/d = b + a_1/10 + a_2/10^2 + r_2/10^2d$. Si $r_2 \neq 0$, se tiene para c/d una aproximación decimal $b.a_1a_2$; pero si $r_2 = 0$, se tiene una representación exacta de c/d como un decimal finito. Así, puede continuarse en esta forma hasta obtener la exactitud deseada. Si el número no se representa por medio de un decimal finito, se ve fácilmente que los dígitos en la parte decimal deben repetirse porque existe solamente un número finito de residuos módulo d. También es posible demostrar que cualquier decimal periódico infinito representa un número racional. Una demostración de este tipo está relacionada, en alguna forma o en otra, con la noción de límite y, por lo tanto, cae fuera de la competencia del álgebra. Sin embargo, el siguiente ejemplo puede ayudar a convencer al estudiante de la plausibilidad de la afirmación anterior. Considérese el decimal periódico $x = 0.141414 \cdots$. Entonces $100x = 14.141414 \cdots = 14 + 0.141414 \cdots = 14 + x$. Así, $99x = 14$ y $x = 14/99$.

Para regresar al problema de construir un número x que represente la hipotenusa del triángulo anterior se procede en la forma siguiente: Se aproxima a x que, generalmente, denotaremos por $\sqrt{2}$, por medio

de números racionales, y se usará la notación decimal. Ahora, 2 se encuentra entre 1^2 y 2^2 y, por lo tanto, entre dos términos consecutivos de la sucesión

$$(1.0)^2, (1.1)^2, (1.2)^2, \cdots, (1.9)^2, 2^2.$$

Se encuentra $(1.4)^2 < 2 < (1.5)^2$. Así, 2 se encuentra entre dos términos consecutivos de la sucesión

$$(1.40)^2, (1.41)^2, (1.42)^2, \cdots, (1.49)^2, (1.50)^2,$$

y se encuentra que $(1.41)^2 < 2 < (1.42)^2$. Puede continuarse este proceso tanto como se desee, obteniendo una aproximación para $\sqrt{2}$ por medio de decimales con el grado de exactitud deseado. Se dice que $\sqrt{2}$ se representa por el decimal infinito (sin repetición) $1.4142\cdots$.

Puede decirse que los números reales consisten de los decimales finitos e infinitos, y, a continuación, interpretaremos esta definición geométricamente. Representemos los enteros por puntos sobre una recta de la manera siguiente: Tomemos dos puntos arbitrarios, nombrando uno 0 y el otro 1. La distancia entre estos dos puntos se toma como unidad de longitud y se establecen intervalos unitarios sobre la recta, nombrando los puntos en la forma acostumbrada:

−4 −3 −2 −1 0 1 2 3 4

Los números racionales, tal y como se aprendió en geometría elemental, también pueden representarse como puntos sobre esta recta. Sin embargo, los números racionales no comprenden todos los puntos sobre la recta porque puede considerarse la hipotenusa de un triángulo rectángulo cuyos catetos son de longitud unitaria y, como se ha visto, este punto no puede representarse por un número racional. Puesto que existen números diferentes a los números racionales que pueden representarse por puntos sobre la recta, hemos extendido nuestro sistema de numeración para incluir estos números y se supone que existe una correspondencia biunívoca entre los números reales y los puntos sobre una recta. Se dice que los puntos que no corresponden a los números racionales, corresponden a los números *irracionales*, y nuestro sistema de los números reales consiste de números racionales e irracionales.

Falta por demostrar que a cada punto de la recta le corresponde un decimal unívocamente determinado, finito o infinito. Podemos hacerlo en la forma siguiente. Sea P cualquier punto sobre la recta. Si está situado entre dos puntos enteros i e $i+1$, se dice que pertenece a este intervalo. Por otra parte, si está situado sobre una marca de división i, pertenece a ambos intervalos $(i-1, i)$ e $(i, i+1)$. Arbitrariamente se dirá que pertenece al intervalo de la derecha $(i, i+1)$ y, en las divisiones posteriores que se harán, también se tomará el intervalo de la derecha si el punto P se encuentra sobre una marca de división. Ahora, considérese que P pertenece al intervalo $(i, i+1)$. Divídase este intervalo en diez partes iguales por medio de los puntos de división $i+1/10, i+2/10, \cdots, i+9/10$ y desígnense estos subintervalos por $0, 1, 2, \cdots, 9$, de izquierda a derecha. Entonces, el subintervalo a_1 tiene los puntos extremos $i + a_1/10$ e $i + (a_1+1)/10$. Supóngase que P pertenece a este subintervalo. Divídase este subintervalo otra vez en diez partes iguales y digamos que P pertenece al nuevo subintervalo a_2, donde a_2 es uno de los enteros $0, 1, 2, \cdots, 9$. Entonces P pertenece al subintervalo cuyos puntos extremos son

$$i + \frac{a_1}{10} + \frac{a_2}{10^2} \quad \text{e} \quad i + \frac{a_1}{10} + \frac{a_2+1}{10^2}.$$

Si se continúa este proceso t veces, P pertenecerá al subintervalo cuyos puntos extremos son

$$i + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_t}{10^t}$$

e

$$i + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_t+1}{10^t}.$$

Ahora que, por supuesto, estos puntos extremos pueden escribirse como $i.a_1a_2\cdots a_t$ e $i.a_1a_2\cdots a_t + 1/10^t$. Se dice que $i.a_1a_2\cdots a_t$ es una aproximación al número que representa a P. Si se continúa indefinidamente este proceso, se obtiene el decimal infinito $i.a_1a_2\cdots a_t\cdots$, del cual se dice que es el número real correspondiente a P.

En nuestro método para encontrar una representación decimal de P, se escogió arbitrariamente el intervalo de la derecha, en cada caso. Por supuesto, podría haberse escogido el intervalo de la izquierda. Esto explica las dos representaciones, por ejemplo, de 2, a saber $2.0000\cdots$ y $1.999\cdots$.

Es evidente que no es necesario escoger la base 10 para nuestra representación. Por ejemplo, podría haberse dividido cada intervalo en

cinco partes iguales. Así, si se hubiera escogido la base 5, la representación posicional de $1/3$ habría sido $0.1313\cdots$ que significa $1/5 + 3/5^2 + 1/5^3 + 3/5^4 \cdots$.

Ejercicios

1. Probar que $\sqrt{3}$ es un número irracional.
2. Encontrar una aproximación decimal para $\sqrt{7}$ a tres cifras decimales por medio del método usado para encontrar una aproximación para $\sqrt{2}$.
3. Expresar $2/9$ como un decimal periódico.
4. Expresar $3/11$ como un decimal periódico.
5. Expresar el decimal periódico $0.343434\cdots$ como una fracción.
6. Expresar el decimal periódico $1.259259\cdots$ como una fracción.
7. Escribir $2/3$ con la base 5 y con la base 6.
8. Escribir 0.425 con la base 7.
9. Escribir 0.312 con la base 9.

4 · NUMEROS COMPLEJOS

La ecuación $x^2 + 2 = 0$ no tiene solución x que sea un número real, porque el cuadrado de cualquier número real es positivo o cero. El deseo de tener soluciones para ese tipo de ecuaciones condujo a una extensión adicional del sistema de numeración, a saber, los números complejos. Definiremos los números complejos en términos de los números reales. Este procedimiento contrasta con el acostumbrado en el álgebra elemental donde los números complejos se introducen mediante la consideración de la raíz cuadrada de -1, y se deduce en tal forma que se tiene la sensación de algo misterioso. (¡Este sentimiento se acentúa por el uso del epíteto "imaginario"!) Aquí se definirán los números complejos como parejas ordenadas de números reales y se verá que son tan "reales" como los enteros que se definieron como parejas ordenadas de números naturales, o los números racionales que se definieron como parejas ordenadas de enteros. En la siguiente sección se relacionará, en una forma obvia, las parejas (a, b) con la notación acostumbrada $a + bi$.

Definición

Un *número complejo* es una pareja ordenada de números reales denotada por (a, b).

Definición de igualdad

Dos números complejos (a, b) y (c, d) son iguales si y solamente si $a = c$ y $b = d$. Nótese que ésta es una igualdad idéntica.

Definición de adición

$$(a, b) + (c, d) = (a + c, b + d).$$

Definición de multiplicación

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Se dejará al estudiante el verificar que la adición y la multiplicación de los números complejos obedecen las leyes conmutativa, asociativa y distributiva.

Identidad para la adición

Puesto que $(a, b) + (0, 0) = (a, b)$, una identidad para la adición es $(0, 0)$.

Inverso aditivo

Puesto que $(a, b) + (-a, -b) = (0, 0)$, se tiene $(-a, -b)$ como un inverso aditivo de (a, b). Se define $-(a, b) = (-a, -b)$ y $(a, b) - (c, d) = (a, b) + (-c, -d)$.

Identidad para la multiplicación

Ya que $(a, b) \cdot (1, 0) = (a, b)$, $(1, 0)$ es un elemento unidad o una identidad para la multiplicación.

Leyes de cancelación

La ley de cancelación para la adición se demuestra rápidamente a partir de la definición de igualdad y suma. La ley de cancelación para la multiplicación puede ponerse en la forma equivalente más fácil de demostrar $(a, b) \cdot (c, d) = (0, 0)$ que implica $(a, b) = (0, 0)$ o $(c, d) = (0, 0)$. Para probar esta ley, supóngase que $(c, d) \neq (0, 0)$. Entonces, se tiene $(ac - bd, ad + bc) = (0, 0)$. De aquí que $ac - bd = 0$, $ad + bc = 0$, y de aquí que $b(c^2 + d^2) = 0$. Por lo tanto, $b = 0$ y $a = 0$. El estudiante debe probar que las dos formas de la ley de cancelación para la multiplicación son equivalentes.

División

Es fácil demostrar que la solución (x, y) de la ecuación $(a, b) = (x, y) \cdot (c, d)$, donde $(c, d) \neq (0, 0)$, está dada por $x = (ac + bd)/(c^2 + d^2)$ y $y = (bc - ad)/(c^2 + d^2)$. Así se encuentra que la división,

excepto por cero, siempre es posible y que el conjunto de números complejos diferentes de cero es cerrado bajo las operaciones racionales.

Ejercicios

1. Probar que la adición de los números complejos obedece las leyes conmutativa y asociativa.
2. Probar que la multiplicación de números complejos obedece las leyes conmutativa y asociativa.
3. Probar que la multiplicación de los números complejos es distributiva respecto de la adición.
4. Probar la ley de cancelación para la adición para los números complejos.
5. Probar que, si $(a, b)(c, d) = (0, 0)$ implica que $(a, b) = (0, 0)$ o $(c, d) = (0, 0)$, entonces $(a, b)(x, y) = (c, d)(x, y)$, con $(x, y) \neq (0, 0)$ implica que $(a, b) = (c, d)$ y recíprocamente.
6. Probar que la ecuación $(a, b) = (x, y) \cdot (c, d)$, donde $(c, d) \neq (0, 0)$ tiene la solución única (x, y), donde $x = (ac + bd)/(c^2 + d^2)$ y $y = (bc - ad)/(c^2 + d^2)$.
7. Probar que existe una identidad *única* para la adición de números complejos.
8. Probar que existe una identidad *única* para la multiplicación de números complejos.
9. Probar que todo número complejo tiene un inverso aditivo *único*.

5 · NUMEROS REALES COMO SUBCONJUNTO DE NUMEROS COMPLEJOS

Puede establecerse un isomoforfismo entre el subconjunto de los números complejos de la forma $(a, 0)$ y los números reales a, de la manera siguiente: Considérese que $(a, 0) \leftrightarrow a$. Ahora, si

$$(a, 0) \leftrightarrow a \qquad \text{y} \qquad (b, 0) \leftrightarrow b,$$

entonces

$$(a, 0) + (b, 0) = (a + b, 0) \leftrightarrow a + b,$$

y

$$(a, 0) \cdot (b, 0) = (ab, 0) \leftrightarrow ab.$$

Ahora, presentaremos la notación más común para el número complejo (a, b), a saber, $a + bi$. Denotemos el número complejo $(0,1)$ por i. Entonces $i^2 = (0, 1) \cdot (0, 1) = (-1, 0)$, el cual corresponde al número real -1. Además $(a, 0) \cdot (0, 1) = (0, a)$ y $(a, b) = (a, 0) + (0, b) = (a, 0) + (0, 1) \cdot (b, 0)$. Ahora se sustituye $(a, 0)$ por su número real correspondiente a y $(b, 0)$ por su número real correspondiente b y se escribe (a, b) simbólicamente como $a + bi$. Cuando se usa la notación $a + bi$ se realiza la adición y la multiplicación como la adición y la multiplicación de polinomios de primer grado en i, pero cuando se presenta, se reemplaza i^2 por -1. Así, $(2 + 3i) + (1 + 4i) = 3 + 7i$ y $(2 + 3i)(1 + 4i) = 2 + 11i + 12i^2 = -10 + 11i$. Obviamente, se tiene un isomorfismo entre las parejas (a, b) y los símbolos $a + bi$ porque, si $(a, b) \leftrightarrow a + bi$ y $(c, d) \leftrightarrow c + di$, entonces

$$(a, b) + (c, d) = (a + c, b + d) \leftrightarrow (a + c) + (b + d)i,$$

y

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc) \leftrightarrow (ac - bd) + (ad + bc)i.$$

De ahora en adelante usaremos la notación acostumbrada $a + bi$, en la cual a y b son números reales, para un número complejo. Si $b = 0$ se dice que el número $a + 0i$ o, simplemente, a, es un número real. Si $a = 0$ y si $b \neq 0$, el número complejo recibe el nombre de número *imaginario puro*.

El número complejo $a - bi$ se llama *conjugado* del número complejo $a + bi$ y se observa que $(a - bi)(a + bi) = a^2 + b^2$ es un número real no negativo. Puede expresarse fácilmente el cociente $(a + bi)/(c + di)$ como un número complejo, multiplicando el numerador y el denominador por $c - di$, obteniendo $(ac + bd)/(c^2 + d^2) + i(bc - ad)/(c^2 + d^2)$. *Nota:* $\sqrt{-1}$ también es un símbolo para i.

Ejercicios

1. Demostrar que el subconjunto de los números complejos de la forma $(0, b)$ no es isomorfo para los números reales.
2. Escribir los números siguientes en la forma $a + bi$: $1 - 2\sqrt{-2}$, $1/i$, $1/(1 + i)$, $(2 + 3i)/(1 + 4i)$, $(2 - \sqrt{-3})(3 + 2i)$, 2, i^3, i^4, i^n.
3. Demostrar que $i^n = 1, -1, i, -i$, de acuerdo con que n sea congruente a $0, 2, 1$ ó 3 módulo 4.

6 · REPRESENTACION GEOMETRICA DE LOS NUMEROS COMPLEJOS

Los números complejos pueden representarse como puntos en un plano. Sean (x, y) las coordenadas cartesianas rectangulares de un punto P en el plano. Se dice que el punto P representa el número complejo $x + yi$. Así, puede asociarse un número complejo a cada punto en el plano, y todo número complejo representa un punto en el plano. Es evidente que los números reales corresponden a los puntos sobre el eje x y que los números imaginarios puros corresponden a los puntos sobre el eje y. Por esta razón, frecuentemente se da el nombre de eje de los reales al eje x, y de eje de los imaginarios al eje y.

También es útil usar coordenadas polares. Sean (ρ, θ) las coordenadas polares de un punto P cuyas coordenadas rectangulares son (x, y) y restrínjase ρ a número positivo o cero. Recordemos que $\rho = \sqrt{x^2 + y^2}$, $x = \rho \cos \theta$, $y = \rho \operatorname{sen} \theta$ y $\tan \theta = y/x$. Ahora, ρ recibe el nombre de *valor absoluto* o *módulo* del número complejo $x + yi$ y θ se llama *ángulo* o *amplitud*. Por ejemplo, el valor absoluto del número complejo $1 - i$ es $\sqrt{2}$ y su ángulo es 315°. De aquí que $1 - i = \sqrt{2}(\cos 315° + i \operatorname{sen} 315°)$. En general, $x + yi = \rho(\cos \theta + i \operatorname{sen} \theta)$, donde ρ es el valor absoluto y θ es el ángulo.

El estudiante no debe caer en el error de leer incorrectamente el ángulo o el valor absoluto de un número complejo cuando encuentra una expresión que es semejante, pero no idéntica, a la forma ordinaria de un número complejo escrito en coordenadas polares. Por ejemplo, el ángulo del número complejo $2(\operatorname{sen} 30° + i \cos 30°)$ no es 30° sino 60°, porque debe escribirse como $2[\cos(90° - 30°) + i \operatorname{sen}(90° - 30°)]$ para que se encuentre en la forma ordinaria. Así, $-2(\cos 60° + i \operatorname{sen} 60°)$ tiene 2 como valor absoluto, pero 240° como ángulo porque

$$-2(\cos 60° + i \operatorname{sen} 60°) = 2[\cos(180° + 60°) + i \operatorname{sen}(180° + 60°)].$$

En la representación de un número complejo en coordenadas polares se observa que, aunque el valor absoluto está unívocamente determinado, el ángulo solamente está determinado dentro de múltiplos enteros de 360° o, en radianes, dentro de múltiplos enteros de 2π. De aquí que *dos números complejos son iguales si y solamente si sus valores absolutos son iguales y si sus ángulos difieren en múltiplos de* 2π. También es útil observar que el conjugado del número $\rho(\cos \theta + i \operatorname{sen} \theta)$ es $\rho[\cos(-\theta) + i \operatorname{sen}(-\theta)] = \rho(\cos \theta - i \operatorname{sen} \theta)$.

Ejercicios

1. Situar en el plano los números complejos siguientes: $2 + 2i$, $-1 - i$, -2, $2i$, $(1 + i)/(1 - i)$, $(2 - 2i)/i$.
2. Encontrar el ángulo y el valor absoluto de cada uno de los números siguientes: $3(\cos 20° + i \operatorname{sen} 20°)$, $-3(\cos 20° + i \operatorname{sen} 20°)$, $-3(\cos 20° + i \operatorname{sen} 20)$, $3(\operatorname{sen} 20° + i \cos 20°)$, $2(\cos 60° - i \operatorname{sen} 60°)$, $2(-\cos 60° + i \operatorname{sen} 60°)$.
3. Encontrar el ángulo y el valor absoluto de cada uno de los números del ejercicio 1 y de los números $-1 + \sqrt{3i}$ e $i/(-1 - \sqrt{3i})$. Escribir estos números en forma polar.

7 · TEOREMA DE DE MOIVRE

El producto y el cociente de dos números complejos, cuando se escriben en forma polar, nos proporcionan algunos resultados interesantes. Sean

$$z_1 = \rho_1(\cos \theta_1 + i \operatorname{sen} \theta_1) \quad \text{y} \quad z_2 = \rho_2(\cos \theta_2 + i \operatorname{sen} \theta_2).$$

entonces

$$\begin{aligned} z_1 z_2 &= \rho_1\rho_2[\cos \theta_1 \cos \theta_2 - \operatorname{sen} \theta_1 \operatorname{sen} \theta_2 + i(\operatorname{sen} \theta_1 \cos \theta_2 + \cos \theta_1 \operatorname{sen} \theta_2)] \\ &= \rho_1\rho_2[\cos(\theta_1 + \theta_2) + i \operatorname{sen}(\theta_1 + \theta_2)]. \end{aligned}$$

Similarmente

$$\begin{aligned} \frac{z_1}{z_2} &= \frac{\rho_1(\cos \theta_1 + i \operatorname{sen} \theta_1)}{\rho_2(\cos \theta_2 + i \operatorname{sen} \theta_2)} \cdot \frac{(\cos \theta_2 - i \operatorname{sen} \theta_2)}{(\cos \theta_2 - i \operatorname{sen} \theta_2)} \\ &= \frac{\rho_1}{\rho_2}[\cos(\theta_1 - \theta_2) + i \operatorname{sen}(\theta_1 - \theta_2)]. \end{aligned}$$

Así se llega al siguiente teorema.

Teorema 1. El valor absoluto del producto de dos números complejos es el producto de sus valores absolutos y el ángulo del producto es la suma de sus ángulos. El valor absoluto del cociente de dos números complejos es el cociente de sus valores absolutos y el ángulo del cociente es el ángulo del numerador menos el ángulo del denominador.

Teorema 2. Teorema de De Moivre. Si n *es un entero positivo*

$$[\rho(\cos \theta + i \operatorname{sen} \theta)]^n = \rho^n(\cos n\theta + i \operatorname{sen} n\theta).$$

Esta fórmula es una extensión inmediata de la fórmula para el producto. Se deja al estudiante demostrarla por inducción.

Ejercicios

1. Probar el teorema 2.
2. Escribir $1/[\rho(\cos \theta + i \operatorname{sen} \theta)]$ en forma polar.
3. Probar que $[\rho(\cos \theta + i \operatorname{sen} \theta)]^{-n} = \rho^{-n}[\cos(-n\theta) + i \operatorname{sen}(-n\theta)]$, donde n es un entero positivo.
4. ¿Cuál es el lugar geométrico de un número complejo a) de valor absoluto fijo, b) de ángulo fijo?
5. Encontrar la forma polar de AB, A/B, A^2/B, y $1/A$, si $A = 2(\cos 30° + i \operatorname{sen} 30°)$ y $B = 4(\cos 50° + i \operatorname{sen} 50°)$.

6. Escribir los números $A = \sqrt{3} - i, B = -\sqrt{3} - i, C = -\sqrt{3} + i$ en forma polar. Encontrar el ángulo y el valor absoluto de cada uno de los siguientes: A^3, B^2/AC.
7. Encontrar el valor de $(1+i)^8$ escribiendo primero $1+i$ en forma polar y a continuación aplicando el teorema de De Moivre. Escribir su respuesta final en la forma $a + bi$. En forma semejante, calcular $(1 - \sqrt{3i})^8$.
8. Puesto que $(\cos\theta + i \operatorname{sen}\theta)^3 = \cos 3\theta + i \operatorname{sen} 3\theta$, aplicar el teorema del binomio para encontrar el valor de $\cos 3\theta$ y $\operatorname{sen} 3\theta$ como funciones de θ.

8 · RAICES *N*-ESIMAS DE UN NUMERO COMPLEJO

Se desea obtener las soluciones z de la ecuación $z^n = A$, donde n es un entero positivo y A un número complejo. Este problema se resuelve fácilmente aplicando coordenadas polares. Sean $z = \rho(\cos\theta + i \operatorname{sen}\theta)$ y $A = r(\cos\phi + i \operatorname{sen}\phi)$. Entonces $z^n = A$ se transforma en

$$\rho^n(\cos n\theta + i \operatorname{sen} n\theta) = r(\cos\phi + i \operatorname{sen}\phi).$$

Recordando que dos números complejos son iguales si y solamente si sus valores absolutos son iguales y sus ángulos difieren en múltiplos enteros de 2π, se tiene $\rho^n = r$ y $n\theta = \phi + 2k\pi$, donde k es un entero. De aquí que $\rho = r^{1/n}$, la raíz n-ésima real positiva de r y $\theta = \phi/n + 2k\pi/n$. Existirán tantos valores diferentes de z como ángulos $\phi/n + 2k\pi/n$ que no sean coterminales. Fácilmente se ve que estos ángulos no son coterminales para los valores $k = 0, 1, 2, \cdots, (n-1)$ porque la diferencia entre cualquier par de ellos es menor que 2π. Para cualquier entero k puede escribirse $k = nq + m$, con $0 \leq m < n$ y se observa que el ángulo $\phi/n + 2k\pi/n$ es coterminal con el ángulo $\phi/n + 2m\pi/n$. Por tanto, existen exactamente n valores distintos de z dados por

$$r^{1/n}[\cos(\phi/n+2k\pi/n) + i \operatorname{sen}(\phi/n+2k\pi/n)], \quad k = 0, 1, 2, \cdots, (n-1).$$

De aquí que existen exactamente n raíces n-ésimas de un número complejo.

EJEMPLO 1. Encontrar las tres raíces cúbicas de $8i$.

Escribir $8i = 8(\cos\pi/2 + i \operatorname{sen}\pi/2)$. Sea $\rho(\cos\theta + i \operatorname{sen}\theta)$ una raíz cúbica. Entonces $\rho^3(\cos 3\theta + i \operatorname{sen} 3\theta) = 8(\cos\pi/2 + i \operatorname{sen}\pi/2)$ y $\rho^3 = 8$ y $3\theta = \pi/2 + 2k\pi$. De aquí que $\rho = 2$ y $\theta = \pi/6 + 2k\pi/3$. Las tres raíces cúbicas de $8i$ son:

$$2\left(\cos\frac{\pi}{6} + i \operatorname{sen}\frac{\pi}{6}\right) = \sqrt{3} + i,$$

$$2\left(\cos\frac{5\pi}{6} + i \operatorname{sen}\frac{5\pi}{6}\right) = -\sqrt{3} + i,$$

$$2\left(\cos\frac{3\pi}{2} + i \operatorname{sen}\frac{3\pi}{2}\right) = -2i.$$

EJEMPLO 2. Encontrar las n raíces n-ésimas de 1.

A estas raíces frecuentemente se les da el nombre de n *raíces n-ésimas de la unidad*. Aplicando la notación presentada en las dos secciones precedentes, se tiene $r = 1$ y $\phi = 0$, y de aquí que $\rho = 1$ y $\theta = 2k\pi/n$. Por lo tanto, las n raíces n-ésimas de la unidad están dadas por $\cos 2k\pi/n + i \operatorname{sen} 2k\pi/n$, $k = 0, 1, \cdots, (n-1)$. Obsérvese que, de acuerdo con el teorema de De Moivre, si hacemos $R = \cos 2\pi/n + i \operatorname{sen} 2\pi/n$, las n raíces n-ésimas de la unidad pueden escribirse $R, R^2, R^3, \cdots R^n$.

Ejercicios

1. Encontrar las tres raíces cúbicas de 8 y simplificar las respuestas.
2. Encontrar las tres raíces cúbicas de 1 y simplificar las respuestas.
3. Encontrar las cuatro raíces cuartas de 1 y escribirlas en forma simplificada. ¿Cuáles de estos resultados son las raíces cuadradas de 1?
4. Encontrar las seis raíces sextas de 1. ¿Cuáles de estos resultados son las raíces cuadradas de 1?; ¿cuáles son las raíces cúbicas de 1?
5. Encontrar las tres raíces cúbicas de -8.
6. Encontrar las dos raíces cuadradas de $(1+i)/\sqrt{2}$.
7. Encontrar las cuatro raíces cuartas de $-16i$.

9 · RAICES *N*-ESIMAS PRIMITIVAS DE LA UNIDAD

En el ejemplo 2, de la sección anterior, se demostró que existen exactamente n números complejos cuyas n-ésimas potencias son iguales a 1, a saber, los números $R = \cos 2\pi/n + i \operatorname{sen} 2\pi/n, R^2, R^3, \cdots, R^n = 1$. En los ejercicios anteriores se observó que algunas de las raíces cuartas de 1 también fueron raíces cuadradas de 1 y que las raíces sextas de 1 contuvieron raíces cuadradas y raíces cúbicas de 1. Es interesante investigar estas observaciones en forma más detenida.

DEFINICIÓN. Un número z es una raíz n-ésima *primitiva* de 1 si $z^n = 1$ y si $z^m \neq 1$, cuando $0 < m < n$.

Teorema 3. Sea R = *cos* 2π/n + 1 *sen* 2π/n. *Si* (k, n) = d, *entonces* R^k *es una raíz* n/d-*ésima primitiva de la unidad.*

Sea $k = k_1 d$ y $n = n_1 d$ de modo que $(k_1, n_1) = 1$. Entonces $R^k = \cos 2k_1 d\pi/n_1 d + i \operatorname{sen} 2k_1 d\pi/n_1 d = \cos 2k_1\pi/n_1 + i \operatorname{sen} 2k_1\pi/n_1$. Ahora, R^k es una raíz $n_1 = n/d$-ésima de la unidad puesto que $(R^k)^{n_1} =$

$\cos 2k_1\pi + i \operatorname{sen} 2k_1\pi = 1$. Por otra parte, R^k es una raíz n/d-ésima primitiva de la unidad, porque si $(R^k)^m = 1 = \cos 2k_1 m\pi/n_1 + i \operatorname{sen} 2k_1 m\pi/n_1$, $k_1 m/n_1$ es un entero. Supuesto que $(n_1, k_1) = 1, n_1 \mid m$. Por tanto, m es un múltiplo de n_1 y el menor valor de m tal que $(R^k)^m = 1$ es n_1.

Corolario 1. R^k *es una raíz* n*-ésima primitiva de la unidad si y solamente si* (k, n) = 1.

Si $(k, n) = 1$, de acuerdo con el teorema, R^k es una raíz $n/1$-ésima $= n$-ésima de la unidad. Inversamente, si R^k es una raíz n-ésima primitiva de la unidad y $(k, n) = d \neq 1$, entonces R^k también es una raíz n/d-ésima primitiva de la unidad; es decir, $(R^k)^{(n/d)} = 1$, lo cual contradice nuestra hipótesis de que R^k es una raíz n-ésima primitiva de la unidad.

Corolario 2. Si U *es cualquier raíz* n*-ésima primitiva de la unidad y* (k, n) = d, *entonces* U^k *es una raíz* n/d*-ésima primitiva de la unidad.*

Ahora, $U = R^t$, donde $(t, n) = 1$. De aquí que $U^k = R^{tk}$ y $(tk, n) = d$. Por lo tanto, puede aplicarse el teorema a R^{tk}.

Corolario 3. Las n *raíces* n*-ésimas de la unidad incluyen todas las raíces* m*-ésimas de la unidad si y solamente si* m *divide a* n.

Si $m \mid n, n = mk$ y $(n, k) = k$. De acuerdo con el teorema 3, R^k es una raíz n/k-ésima $= m$-ésima primitiva de la unidad. Así que $R^k, R^{2k}, \cdots, R^{mk}$ son todas raíces m-ésimas de la unidad puesto que $(R^{jk})^m = (R^{km})^j = 1$. De aquí que todas las raíces m-ésimas de la unidad están incluidas entre las raíces n-ésimas. Por otra parte, si todas las raíces m-ésimas de la unidad están incluidas entre las raíces n-ésimas, entonces la raíz m-ésima primitiva $\cos 2\pi/m + i \operatorname{sen} 2\pi/m = R^v$. De acuerdo con el teorema 3, si $(v, n) = d, R^v$ es una raíz n/d-ésima primitiva de la unidad. De aquí que $n/d = m$ y $n = md$.

Ejercicios

1. Encontrar las raíces cúbicas primitivas de 1.
2. Encontrar las raíces 8-avas primitivas de 1.
3. Encontrar las raíces 5-as primitivas de 1.
4. Demostrar que si p es primo, existen exactamente $p - 1$ raíces p-ésimas primitivas de 1.
5. ¿Cuántas raíces n-ésimas reales de 1 existen?
6. ¿Cuántas raíces n-ésimas reales de un número real positivo existen?
7. ¿Cuántas raíces n-ésimas reales de un número real negativo existen?

8. ¿Cuántas raíces p^2-ésimas primitivas de 1 existen si p es primo?
9. Encontrar las doce raíces 12-as de 1 ¿Cuáles dentro de ellas son raíces cuadradas primitivas, raíces cúbicas primitivas, raíces cuartas primitivas, raíces sextas primitivas?
10. Si $R = \cos 2\pi/7 + i \operatorname{sen} 2\pi/7$, expresar R^{-1}, R^{-4}, R^{-10}, como R^k, donde $0 < k < 7$.
11. Si $\omega = -1/2 + i\sqrt{3}/2$, encontrar el valor de $\omega^n + \omega^{-n}$ para todos los enteros positivos n.

3 Teoría elemental de grupos

1 · DEFINICION

Ahora empezaremos el estudio de los sistemas matemáticos que pertenecen principalmente a la división de las matemáticas llamada álgebra. En cualquier sistema matemático se tiene, primero que nada, un conjunto S de elementos que denotaremos por $a, b, c, \cdots$ y una relación de igualdad o equivalencia entre pares de elementos. Hemos tenido algunos ejemplos de tales relaciones de igualdad, a saber, la igualdad idéntica ordinaria, la igualdad usada para definir los enteros, la igualdad usada para definir los números racionales y la congruencia de los enteros. En todos los sistemas algebraicos que se estudiarán en adelante, se supondrá, sin mención posterior, que existe una relación de igualdad.

Además de los elementos y de una relación de equivalencia, en un sistema algebraico se tienen una o más operaciones sobre un par de elementos del conjunto S para producir un tercer elemento de S. Las operaciones de este tipo reciben el nombre de *operaciones binarias*. En general, una operación binaria $\circ$ sobre un conjunto de elementos S es una regla que asigna a cada pareja ordenada de elementos a, b, en S, un elemento único c en S, y se escribe $a \circ b = c$. La operación binaria estará bien definida si, cuando se sustituyen a o b, o tanto a como b, por elementos respectivamente iguales a ellos, c se reemplaza por un elemento igual a él. Operaciones binarias bien conocidas son las de adición y multiplicación de los números.

Uno de los sistemas algebraicos más sencillo es el grupo. Daremos la siguiente definición.

Postulados para un grupo. Un conjunto S de elementos $a, b, c, \cdots$ forma un grupo respecto de la operación $\circ$ si se cumplen las propiedades:

1. Si a y b están en S, entonces $a \circ b$ está en S (cerradura).
2. Para todo a, b, c, en S, $a \circ (b \circ c) = (a \circ b) \circ c$ (ley asociativa).
3. Existe en S un elemento i, llamado *identidad izquierda*, tal que $i \circ a = a$ para todo a en S.
4. Para todo a en S, la ecuación $x \circ a = i$ tiene una solución x en S. La solución x recibe el nombre de *inverso izquierdo* de a y se denota por a^{-1}.

El estudiante debe observar que, mientras que una identidad izquierda i es la misma para todos los elementos a en S, un inverso izquierdo de un elemento a está determinado por el elemento a dado; es decir, existe una identidad izquierda "universal", pero no un inverso izquierdo "universal". Aunque en los ejemplos y ejercicios siguientes todas las operaciones de grupo obedecen la ley conmutativa, el estudiante no debe concluir que los postulados establecen que las operaciones del grupo son conmutativas. Si $a \circ b = b \circ a$ para toda a y b, en el grupo, el grupo recibe el nombre de grupo *abeliano* o *conmutativo*. Posteriormente se encontrarán ejemplos de grupos no abelianos.

EJEMPLOS. Los principales ejemplos de grupos que hasta ahora ha encontrado el estudiante se tienen en el sistema de numeración.

a. Los enteros forman un grupo respecto de la adición, pero no respecto de la multiplicación.

b. Las clases de residuos módulo 3 forman un grupo respecto de la adición y las clases de residuos, diferentes de cero, módulo 3 forman un grupo respecto de la multiplicación.

c. Los números $i, -1, -i$ y 1 forman un grupo respecto de la multiplicación.

Ejercicios

En cada uno de los ejercicios siguientes comprobar todos los postulados para formar un grupo.

1. ¿Forman un grupo los enteros pares respecto de la adición? ¿Forman un grupo los enteros impares respecto de la adición?
2. ¿Forman un grupo los números reales positivos respecto de la multiplicación? ¿Forman un grupo todos los números racionales respecto de la multiplicación?
3. ¿Forman un grupo los números irracionales positivos respecto de la multiplicación?
4. Sea $a \circ b = a - b$, donde a y b son enteros. ¿Forman los enteros un grupo respecto de esta operación?
5. Probar que las clases de residuos, diferentes de cero, módulo 5 forman un grupo respecto de la multiplicación.
6. Probar que las clases de residuos módulo 4 no forman un grupo respecto de la multiplicación.
7. Demostrar que todos los enteros de la forma $3m$, donde m es un entero, forman un grupo respecto de la adición.

8. Demostrar que todos los múltiplos enteros de un entero fijo k forman un grupo respecto de la adición.
9. Si las clases de residuos módulo 7 se denotan por los enteros 0, 1, 2, 3, 4, 5, ¿cuáles de los conjuntos siguientes forman un grupo respecto de la multiplicación: (a) [1, 2, 4]; (b) [0, 1, 2, 3, 4, 5, 6]; (c) [1, 6]; (d) [1, 3, 4, 5]; (e) [1, 2, 3, 4, 5, 6] ?
10. Demostrar que las raíces quintas de la unidad forman un grupo respecto de la multiplicación.
11. Demostrar que las n raíces n-ésimas de la unidad forman un grupo respecto de la multiplicación.
12. Demostrar que las clases de residuos módulo m forman un grupo respecto de la adición.
13. Demostrar que las clases de residuos diferentes de cero módulo p forman un grupo respecto de la multiplicación si y solamente si p es primo.
14. Probar que las clases de residuos C_a módulo m tales que $(a, m) = 1$ forman un grupo respecto de la multiplicación.

2 · PROPIEDADES ELEMENTALES

Ahora se probarán algunos teoremas sencillos directamente a partir de la definición de grupo. En los teoremas que siguen ab significará $a \circ b$ y la operación binaria se llamará multiplicación.

Teorema 1. Si a, b, c *están en un grupo,* ab = ac *implica* b = c.

Se multiplica la ecuación $ab = ac$ a la izquierda por un inverso izquierdo a^{-1} de a y se aplica la ley asociativa, se obtiene $(a^{-1}a)b = (a^{-1}a)c$, lo cual conduce a $ib = ic$ y, finalmente, a $b = c$.

Teorema 2. Un elemento identidad izquierda en un grupo, también es elemento identidad derecha, es decir, ia = ai = a *para todo* a *en el grupo.*

Sea a^{-1} un inverso izquierdo de a. Entonces $a^{-1}(ai) = (a^{-1}a)i = ii = i = a^{-1}a$. Aplicando el teorema 1, se tiene $ai = a$. De aquí en adelante dejaremos de usar los calificativos izquierda y derecha, y para mencionar el elemento i diremos simplemente identidad.

Teorema 3. Un inverso izquierdo a^{-1} *de un elemento* a *en un grupo, también es un inverso derecho de* a, *es decir,* $a^{-1}a = aa^{-1} = i$.

Ahora, $a^{-1}(aa^{-1}) = (a^{-1}a)a^{-1} = ia^{-1} = a^{-1} = a^{-1}i$. Por lo tanto, de acuerdo con el teorema 1, $aa^{-1} = i$. A partir de este momento nos referiremos a a^{-1} usando el término inverso.

Corolario. Si a, b, c *son elementos en un grupo, entonces* ba = ca *implica* b = c.

La demostración es la misma que para el teorema 1 porque ahora es posible multiplicar a la derecha por un inverso de a y obtener $b = c$.

Teorema 4. Si a *y* b *son elementos en un grupo, las ecuaciones* ax = b *y* ya = b, *respectivamente, tienen soluciones únicas* x *y* y *en el grupo.*

Rápidamente se ve que una solución de $ax = b$ es $a^{-1}b$ y que una solución de $ya = b$ es ba^{-1}, puesto que $a(a^{-1}b) = (aa^{-1})b = ib = b$ y $(ba^{-1})a = b(a^{-1}a) = bi = b$. Las soluciones son únicas porque si x' y y' son unas segundas soluciones, entonces $ax = ax'$ y $ya = y'a$, dando $x = x'$ y $y = y'$.

Corolario 1. El elemento identidad en un grupo es único.

La identidad es la solución única de la ecuación $ax = a$.

Corolario 2. El inverso de un elemento en un grupo es único.

El inverso a^{-1} de a es la solución única de la ecuación $ax = i$.

Corolario 3. El inverso de a^{-1} *es* a.

Es obvio que el elemento a es la solución de la ecuación $a^{-1}x = i$. De aquí se observa que $(a^{-1})^{-1} = a$.

Teorema 5. El inverso de un producto es el producto de los inversos en orden contrario, es decir, $(ab)^{-1} = b^{-1}a^{-1}$.

Se tiene $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(ib) = b^{-1}b = i$.

Ejercicios

1. Si a, b, c son elementos de un grupo, probar que la ecuación $xaxba = xbc$ tiene una solución única.
2. Probar que, si x es un elemento de un grupo y $xx = x$, entonces $x = i$, el elemento identidad del grupo.
3. Demostrar que, en un grupo con un número par de elementos, además del elemento identidad existe un elemento que es su propio inverso.
4. Probar que $(ab)(ab) = (aa)(bb)$ para todos los elementos a y b de un grupo G si y solamente si G es un grupo abeliano.
5. Sea S un conjunto de elementos $a, b, c, \cdots$ que satisface los postulados 1 y 2 y que, además, tiene la propiedad de que todas las ecuaciones $xa = b$ y $ay = b$ tienen soluciones x y y en S. Probar que S es un grupo.

3 · PERMUTACIONES

Hasta el momento, todas las operaciones binarias que hemos encontrado han obedecido la ley conmutativa. Ahora se definirán algunos símbolos y se encontrará que la regla para combinarlos no obedece la ley conmutativa.

La operación de sustituir cada uno de los n enteros $1, 2, \cdots, n$ por uno de ellos, de modo que dos enteros distintos no se reemplacen por el mismo entero, recibe el nombre de *permutación* realizada en los enteros $1, 2, \cdots, n$. Una permutación reemplaza cualquier arreglo de los n enteros por un nuevo arreglo. Es obvio que los n enteros simplemente forman una notación conveniente para cualquier conjunto de n símbolos. Introduciremos un símbolo para una permutación. Sea $j_1, j_2, \cdots, j_n$ cualquier arreglo del conjunto de enteros $1, 2, \cdots, n$. El símbolo

$$p = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$$

dará a entender que debe sustituirse 1 por j_1, 2 por j_2, etc., hasta que, finalmente, se reemplaza n por j_n. Este símbolo denota una permutación. Nótese que el orden de las columnas en el símbolo es inmaterial.

Se define el producto de dos permutaciones $p \circ q$ o, tal y como se escribirá, pq, indicando que primero se efectúa p y a continuación q. Así, si

$$q = \begin{pmatrix} j_1 & j_2 & \cdots & j_n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix},$$

donde $k_1, k_2, \cdots, k_n$ son $1, 2, \cdots, n$ en algún orden,

$$pq = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix}.$$

En general, esta multiplicación no es conmutativa porque si, por ejemplo,

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{y} \quad q = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

entonces

$$pq = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{y} \quad qp = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Sin embargo, puede probarse que la multiplicación de permutaciones es asociativa. Sean p y q las permutaciones de n símbolos dadas anteriormente, y sea

$$r = \begin{pmatrix} k_1 & k_2 & \cdots & k_n \\ m_1 & m_2 & \cdots & m_n \end{pmatrix},$$

donde $m_1, m_2, \cdots, m_n$ son los enteros $1, 2, \cdots, n$ en algún orden. Usando el valor de pq, ya encontrado, se tiene

$$(pq)r = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ m_1 & m_2 & m_3 & \cdots & m_n \end{pmatrix},$$

mientras que

$$qr = \begin{pmatrix} j_1 & j_2 & \cdots & j_n \\ m_1 & m_2 & \cdots & m_n \end{pmatrix} \quad \text{y} \quad p(qr) = \begin{pmatrix} 1 & 2 & \cdots & n \\ m_1 & m_2 & \cdots & m_n \end{pmatrix}.$$

Por lo tanto, $(pq)r = p(qr)$.

Para todo arreglo de $1, 2, 3, \cdots, n$, puede escribirse una permutación diferente. Puesto que existen $n!$ arreglos diferentes de n símbolos, existen $n!$ permutaciones diferentes para n símbolos, las cuales pueden escribirse insertando en la segunda línea de p los $n!$ arreglos diferentes de $1, 2, \cdots, n$.

Teorema 6. Las n! *permutaciones diferentes sobre* n *símbolos forman un grupo respecto de la multiplicación de permutaciones.*

Puesto que todas las permutaciones sobre n símbolos se incluyen en el conjunto, el conjunto es cerrado respecto de la multiplicación de permutaciones. Ya se demostró que esta multiplicación es asociativa. La identidad es

$$i = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix},$$

porque es obvio que tiene la propiedad $ip = pi = p$ para toda permutación p sobre los enteros $1, 2, \cdots, n$. Sea p la permutación dada anteriormente. Entonces la inversa de p es

$$p^{-1} = \begin{pmatrix} j_1 & j_2 & \cdots & j_n \\ 1 & 2 & \cdots & n \end{pmatrix},$$

puesto que $pp^{-1} = p^{-1}p = i$.

Este grupo recibe el nombre de *grupo simétrico* para n símbolos y juega un papel importante en muchas aplicaciones de la teoría de grupos.

Notación cíclica

Es conveniente escribir las permutaciones en lo que se llama notación cíclica o en ciclos. Por ejemplo, la permutación

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

puede escribirse simplemente como (1234). El nuevo símbolo, llamado *ciclo*, se lee en orden cíclico de izquierda a derecha de la manera siguiente: 1 se sustituye por 2, 2 por 3, 3 por 4 y 4 por 1. Obsérvese que $(1234) = (2341) = (3412) = (4123)$.

En la misma forma, la permutación

$$t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

se escribe $(123)(45)$, y la permutación

$$u = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

se escribe como $(1)(23)$ o, simplemente, como (23). Se entiende que cuando se omite un símbolo se reemplaza por él mismo. Ahora ha quedado razonablemente claro que cualquier permutación puede escribirse

como un producto de ciclos, los cuales no tienen símbolos comunes (ciclos *ajenos*).

Ejercicios

1. Escribir las 4! permutaciones sobre 4 símbolos en la notación de las dos líneas y en la notación cíclica.
2. Realizar las siguientes multiplicaciones de permutaciones: (a) (1245)(32154); (b) (123)(243)(134); (c) (15624)(6321).
3. Encontrar el inverso de cada uno de los productos del ejercicio 2.
4. Realizar las siguientes multiplicaciones de permutaciones:

a. (243)(13),	b. (4312)(2341),	c. (43)(3421),	d. (431)(231),
e. (12)(34)(24),	f. (132)(1342),	g. (34)(143),	h. (1432)(14),
i. (1324)(134),	j. (1423)(24),	k. (142)(23),	l. (234)(143).

5. Si $a = (123456)$, encontrar a^2, a^3, a^4, a^5, a^6.
6. Demostrar que las seis permutaciones del ejercicio 5 forman un grupo respecto de la multiplicación de permutaciones.
7. Escribir los productos siguientes como productos de ciclos ajenos: (*a*) (132)(567)(261)(45); (*b*) (1234)(67)(1357)(136); (*c*) (24)(132)(45)(24).

4 · PERMUTACIONES PARES E IMPARES

DEFINICIÓN. Una permutación que solamente desplaza dos símbolos se llama *transposición*.

Teorema 7. Un ciclo de n *símbolos puede escribirse como un producto de* n − 1 *transposiciones.*

Este hecho se ve claramente cuando se exhibe la identidad

$$(1234\cdots n) = (12)(13)(14)\cdots(1n).$$

De aquí que toda permutación puede escribirse como un producto de transposiciones puesto que así puede escribirse cada uno de sus ciclos.

Una permutación puede escribirse en muchas formas como un producto de transposiciones. Por ejemplo, $(123) = (12)(13)$, asimismo, $(123) = (13)(12)(13)(12)$. Sin embargo, para una permutación dada, el número de transposiciones siempre es par o siempre es impar. Esto se prueba en el teorema siguiente.

Teorema 8. Considérese una permutación p *escrita como un producto de* a *transposiciones y como un producto de* b *transposiciones. Entonces* $a \equiv b$ (*mod* 2).

Para probar este teorema considérese la llamada función alternante A sobre los n símbolos distintos $x_1, x_2, \cdots, x_n$, la cual es el producto de los $n(n-1)/2$ factores $(x_i - x_j), i < j$. Por lo tanto

$$\begin{aligned} A = \prod_{i<j}^{n} (x_i - x_j) &= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)\cdots(x_1 - x_n) \\ &\quad (x_2 - x_3)(x_2 - x_4)\cdots(x_2 - x_n) \\ &\quad (x_3 - x_4)\cdots(x_3 - x_n) \\ &\quad \cdots\cdots\cdots\cdots \\ &\quad (x_{n-1} - x_n). \end{aligned}$$

Se opera sobre A por la transposición $t = (x_i x_j)$, donde $i < j$. Todos los factores de A, que no contienen a x_i ni a x_j, no se alteran cuando se opera sobre A mediante la permutación t, pero el factor $(x_i - x_j)$ de A se transforma en su negativo. Los factores de A que contienen a x_i o a x_j, pero no tanto a x_i como a x_j, pueden agruparse en pares de productos $\pm(x_k - x_i)(x_k - x_j)$, donde $k \neq i, j$. Tales productos no cambian cuando se opera sobre A mediante una transposición t, se transforma en $-A$.

Ahora, se opera sobre A mediante la permutación p, la cual puede escribirse como un producto de a transposiciones y también como un producto de b transposiciones. Operando sobre A mediante p, cuando se escribe como un producto de a transposiciones, se obtiene $(-1)^a A$, mientras que, operando sobre A mediante p, cuando se escribe como un producto de b transposiciones, se obtiene $(-1)^b A$. Puesto que p es la misma permutación, no importa como se escriba, $(-1)^a A = (-1)^b A$, con lo cual se demuestra que $a \equiv b \pmod 2$.

DEFINICIÓN. Se dice que una permutación es una permutación *par* o una permutación *impar* de acuerdo con que pueda escribirse como un producto de un número par o un número impar de transposiciones.

Teorema 9. De las n! *permutaciones sobre* n *símbolos,* n!/2 *son permutaciones pares y* n!/2 *son permutaciones impares.*

De las $n!$ permutaciones sobre n símbolos, sean $e_1, e_2, \cdots, e_r$ las permutaciones pares y $o_1, o_2, \cdots, o_s$ las permutaciones impares. Multiplíquese cada una de estas permutaciones a la izquierda por la transposición t (que, por supuesto, es una permutación impar). Las $te_j, j = 1, 2, \cdots, s$ son permutaciones impares, puesto que cada e_j ha sido multiplicada

por la transposición t, mientras que las $to_k, k = 1, 2, \cdots, r$ son permutaciones pares porque cada o_k ha sido multiplicada por la transposición t. Ahora, se probará que las te_j y las to_k son otra vez las $n!$ permutaciones. Puesto que, evidentemente, ninguna permutación par puede ser igual a una permutación impar, únicamente es necesario probar que no puede tenerse $te_v = te_w$ *cuando* $e_v \neq e_w$, y que tampoco $to_v = to_w$ cuando $o_v \neq o_w$. Este hecho puede concluirse directamente a partir de la ley de cancelación, puesto que $te_v = te_w$ implica $e_v = e_w$ y $to_v = to_w$ implica $o_v = o_w$. Así que las $te_j, j = 1, 2, \cdots, s$ son las permutaciones $o_k, k = 1, 2, \cdots, r$ en algún orden, y de aquí que $s = r = n!/2$.

Ejercicios

1. Demostrar que la identidad es una permutación par.
2. Demostrar que un ciclo que contiene un número impar de símbolos es una permutación par, mientras que un ciclo que contiene un número par de símbolos es una permutación impar.
3. Escribir cada una de las $4!$ permutaciones sobre 4 símbolos como un producto de transposiciones. ¿Cuáles son permutaciones pares y cuáles son permutaciones impares?
4. Si p es una permutación par, demostrar que p^{-1} es una permutación par.
5. Probar que las $n!/2$ permutaciones pares sobre n símbolos forman un grupo respecto de la multiplicación de permutaciones. Este grupo se conoce como el *grupo alternante* sobre n símbolos.
6. Probar que toda permutación par es un ciclo de longitud tres o puede expresarse como un producto de ciclos de longitud tres.

5 · ISOMORFISMO

DEFINICIÓN. Un *isomorfismo* entre dos grupos G y G' es una correspondencia biunívoca $a \leftrightarrow a'$ entre los elementos a y a' de G y G', respectivamente, tal que si $a \leftrightarrow a'$ y $b \leftrightarrow b'$, entonces $ab \leftrightarrow a'b'$. En el isomorfismo, a' es la *imagen* de a.

Nótese que un isomorfismo no exige que la operación, o ley de combinación, para los elementos de cada grupo, sea la misma. Hemos omitido el símbolo para la operación en la definición, pero si $\circ$ es la operación para G y si $\circ'$ es la operación para G', entonces la condición para un isomorfismo se lee $a' \circ' b' = (a \circ b)'$.

EJEMPLO. Sea G el grupo multiplicativo de las raíces cuartas de la unidad y sea G' el grupo aditivo de las clases de residuos módulo 4 (cuyos elementos se denotarán por $0, 1, 2, 3$ en lugar de C_0, C_1, C_2 y C_3, respectivamente). Entonces, puede establecerse un isomorfismo entre G y G' en las dos formas siguientes:

G		G'		G		G'
1	$\leftrightarrow$	0		1	$\leftrightarrow$	0
i	$\leftrightarrow$	1		i	$\leftrightarrow$	3
-1	$\leftrightarrow$	2		-1	$\leftrightarrow$	2
$-i$	$\leftrightarrow$	3;		$-i$	$\leftrightarrow$	1.

El número de formas en que puede establecerse un isomorfismo entre dos grupos depende de la estructura del grupo. Sin embargo, no importa cómo se establezca el isomorfismo, debe observarse el hecho siguiente. Escribir la llamada "tabla de multiplicación" para cada grupo G y G'.

G:

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

G':

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Para cada isomorfismo se ve que las dos tablas de multiplicación se vuelven idénticas si cada símbolo de G se reemplaza por su imagen en G', e inversamente.

Teorema 10. En un isomorfismo entre dos grupos G *y* G', *las identidades corresponden y si* a' *en* G' *es la imagen de* a *en* G, *entonces la imagen de* a^{-1} *es* $(a')^{-1}$.

Primero probaremos que las identidades se corresponden. Sea i la identidad de G e i' la identidad de G'. Supóngase que $i \leftrightarrow a'$ en G' y sea x cualquier elemento de G y x' su imagen en G'. Entonces, puesto que $ix = x$, se tiene, a partir de la definición de isomorfismo, $a'x' = x'$ para toda x' de G. De aquí que a' es una identidad para G' y, ya que la identidad es única, $a' = i'$.

A continuación se probará que los elementos inversos se corresponden. Considérese que $a \leftrightarrow a'$ y $a^{-1} \leftrightarrow b'$. Puesto que $a^{-1}a = i$ se tiene, de acuerdo con la definición de isomorfismo, $b'a' = i'$ y como el inverso de un elemento es único, $b' = (a')^{-1}$.

Ejercicios

1. Establecer un isomorfismo entre el grupo multiplicativo de las raíces cuartas de la unidad y el grupo de permutaciones cuyos elementos son $i = (1)(2)\cdot(3)(4)$, (1234), $(13)(24)$, (1432).
2. ¿Es posible establecer un isomorfismo entre el grupo multiplicativo de las

raíces cuartas de la unidad y el grupo de permutaciones cuyos elementos son $i = (1)(2)(3)(4), (12)(34), (13)(24), (14)(23)$?

3. Establecer un isomorfismo entre el grupo multiplicativo de las cinco raíces quintas de la unidad y el grupo de permutaciones cuyos elementos son $i = (1)(2)(3)(4)(5), (12345), (13524), (14253), (15432)$.
4. ¿Es isomorfo el grupo multiplicativo de los números reales diferentes de cero para el grupo aditivo de todos los números reales?

6 · GRUPOS CICLICOS

Potencias enteras de un elemento

Se definirán las potencias enteras de un elemento a de un grupo. Por a^m donde m es un entero positivo, se entenderá $a \circ a \circ \cdots \circ a$ hasta m factores. (Si la operación se llama adición a^m generalmente se denotará por $ma = a + a + \cdots + a$ (m términos), donde se entiende que m no es necesariamente un elemento de un grupo y, generalmente, no lo es). Obsérvese que esta forma de escribir m factores sin paréntesis solamente es posible porque un "producto" de m factores es independiente de la manera en que se agrupen los factores. Esta ley asociativa generalizada puede probarse por inducción partiendo de la ley asociativa. Además, se define $a^0 = i$, la identidad, y $a^{-m} = (a^{-1})^m$, donde m es un entero positivo. Con estas definiciones es fácil probar el teorema siguiente.

Teorema 11. Para todo elemento a *en un grupo, (1)* $a^r \circ a^s = a^{r+s}$, *y (2)* $(a^r)^s = a^{rs}$.

Primero estableceremos (1): Para exponentes enteros positivos esta ley simplemente es una aplicación de la definición porque $a^r \circ a^s = a \circ a \circ \cdots \circ a$ hasta $r + s$ factores. De acuerdo con la definición de a^0 (1) se cumple si uno o ambos exponentes son cero. En caso de que $r = -m, s = -n$, m y n enteros positivos, se tiene

$$
\begin{aligned}
a^r \circ a^s = a^{-m} \circ a^{-n} &= (a^{-1})^m \circ (a^{-1})^n && \text{por definición,}\\
&= (a^{-1})^{m+n} && \text{de acuerdo con (1) para exponentes positivos,}\\
&= a^{-(m+n)} && \text{por definición,}\\
&= a^{r+s}.
\end{aligned}
$$

Si $r = -m$ y si $s = n$, donde m y n son enteros positivos, se tiene, aplicando la definición de los exponentes negativos,

$$a^r \circ a^s = a^{-m} \circ a^n = a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1} \circ a \circ a \cdots \circ a$$

(m factores a^{-1} y n factores a),

$$
\begin{aligned}
&= a^{n-m}, && m \le n,\\
&= (a^{-1})^{m-n}, && m > n,\\
&= a^{-m+n} = a^{r+s}.
\end{aligned}
$$

Por lo tanto, se han investigado todos los casos y (1) se cumple para todos los exponentes enteros.

A continuación se establecerá (2): Una vez más es obvio que (2) se cumple si cualquiera o ambos exponentes son cero. Si $s > 0$, entonces

$$
\begin{aligned}
(a^r)^s &= a^r \circ a^r \circ \cdots \circ a^r && \text{hasta } s \text{ factores,}\\
&= a^{rs} && \text{por (1).}
\end{aligned}
$$

Si $s = -n$, donde n es un entero positivo, por definición, se tiene

$$(a^r)^s = (a^r)^{-n} = [(a^r)^{-1}]^n.$$

Ahora, $(a^r)^{-1}$ es el inverso de a^r y, por (1), $a^r \circ a^{-r} = a^0$ De aquí que, puesto que el inverso de un elemento es único, $(a^r)^{-1} = a^{-r}$. Por lo tanto

$$
\begin{aligned}
[(a^r)^{-1}]^n = (a^{-r})^n &= a^{-rn} && \text{por (1),}\\
&= a^{rs}.
\end{aligned}
$$

En general, $(ab)^r \neq a^r b^r$. En particular, si $ab \neq ba$, $(ab)^2 \neq a^2 b^2$. Porque si $(ab)^2 = a^2 b^2$, entonces $abab = aabb$ y, aplicando el teorema 1 y el corolario al teorema 3, se tiene $ab = ba$.

Definición de grupo cíclico

Obsérvese que las definiciones anteriores de las potencias enteras de un elemento a de un grupo, junto con el teorema 11, prueban que las potencias enteras de cualquier elemento a de un grupo forman un grupo. Un grupo que solamente consiste de las potencias de un elemento a recibe el nombre de grupo cíclico. Ese elemento a es el *generador* del grupo cíclico.

Definición del orden de un elemento

Se dice que un elemento a en un grupo es de orden n, si n es el menor entero positivo tal que $a^n = i$, la identidad. Se dice que un elemento a es de orden cero si ninguna potencia positiva de a es la identidad; es decir, a^0 es la única potencia de a que es la identidad.

Orden de un grupo

Un grupo que consiste de un número finito de elementos se llama grupo *finito*, mientras que un grupo que tiene un número infinitamente grande de elementos es un grupo *infinito*. El orden de un grupo finito es el número de sus elementos. Se dice que un grupo infinito tiene el orden cero.

Teorema 12. Si un generador a *de un grupo cíclico* G *es de orden cero,* G *es isomorfo para el grupo aditivo de los enteros. Si un generador* a *de* G *es de orden* $n > 0$, G *es isomorfo para el grupo aditivo de clases de residuos módulo* n.

Primero se probará que si el orden de a es cero, no existen dos potencias de a que sean iguales. Puesto que, si $a^s = a^t$ cuando $s \neq t$, entonces $a^s a^{-t} = a^t a^{-t} = i$, y $a^{s-t} = i = a^{t-s}$ y, por lo tanto, puesto que ya sea $s - t$ ó $t - s$ es positivo, una potencia positiva de a es igual a i. Ahora, puesto que $a^s a^t = a^{s+t}$, la correspondencia $a^s \leftrightarrow s$ es un isomorfismo, y G es isomorfo para el grupo aditivo de los enteros.

Ahora, sea a de orden $n > 0$, se probará que G consiste solamente de n elementos distintos. Para cualquier entero s se tiene $s = nq + r$, donde $0 \leq r < n$. Por lo tanto, cualquier elemento a^s de G puede escribirse $a^s = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = ia^r = a^r$. Por lo tanto, existen cuando mucho n elementos distintos $a, a^2, \cdots, a^{n-1}, a^n = i$. Si $x > y$, donde $0 < x < n$ y $0 < y < n$, entonces $a^x \neq a^y$, porque si $a^x = a^y$, $a^{x-y} = i$, pero $0 < x - y < n$, contrario a la definición del orden de a. Por lo tanto, existen por lo menos n elementos distintos. De aquí que existen en el grupo exactamente n elementos distintos $a, a^2, a^3, \cdots, a^{n-1}, a^n = a^0 = i$. Denotando las clases de residuos módulo n por $C_0, C_1, C_2, \cdots, C_{n-1}$, se ve que la correspondencia $a^s \leftrightarrow C_s$ es un isomorfismo entre el grupo aditivo de las clases de residuos módulo n y G, porque, si $a^t \leftrightarrow C_t$, entonces $a^s a^t = a^{s+t} = a^r \leftrightarrow C_s + C_t = C_r$, donde $s + t \equiv r \pmod{n}$.

Ejercicios

1. Demostrar que las permutaciones siguienes forman un grupo: $i = (1)(2)(3)(4)$, (1234), $(13)(24)$, (1432), (13), (24), $(14)(23)$, $(12)(34)$. ¿Es isomorfo este grupo para el grupo multiplicativo de las raíces octavas de la unidad? ¿Es un grupo cíclico el grupo de permutaciones? ¿Es un grupo cíclico el grupo multiplicativo de las raíces octavas de la unidad?
2. En los problemas siguientes, denotar las clases de residuos módulo m por $0, 1, 2, \cdots, m - 1$.
   a. ¿Es cíclico el grupo multiplicativo 1, 2, 3, 4, 5, 6 módulo 7?
   b. ¿Es cíclico el grupo multiplicativo 1, 3, 5, 7 módulo 8?
   c. ¿Es cíclico el grupo multiplicativo 1, 2, 4, 5, 7, 8 módulo 9?

3. ¿Es cíclico el grupo aditivo de los múltiplos enteros de 5?
4. Establecer un isomorfismo en el mayor número posible de formas entre el grupo multiplicativo de las raíces sextas de la unidad y el grupo aditivo de las clases de residuos módulo 6.
5. ¿Cuántos elementos del grupo cíclico de orden 6 pueden usarse como generadores del grupo?
6. Demostrar que un grupo abeliano de orden 6 que contiene un elemento de orden 3, necesariamente es un grupo cíclico.
7. Probar que, si un grupo cíclico G se genera por un elemento a de orden m, a^k genera a G si y solamente si $(k, m) = 1$.
8. Si un grupo cíclico G se genera por un elemento a de orden m, encontrar el orden de cualquier elemento a^k de G.

7 · SUBGRUPOS

DEFINICIONES. Un subconjunto S de elementos de un grupo G que es así mismo un grupo, recibe el nombre de *subgrupo* de G. Se entiende que la ley de combinación de los elementos es la misma que para el propio grupo. Tanto la identidad sola como el mismo grupo G satisfacen esta definición. Los subgrupos, que no son la identidad y el grupo mismo, se llaman subgrupos *propios*, éstos son los que nos interesan principalmente.

Teorema 13. Las condiciones necesarias y suficientes para que un subconjunto S *de elementos de un grupo* G *forme un grupo son: (1) si* a *y* b *están en* S, *entonces* ab *está en* S *y (2) si* a *está en* S, *entonces* a^{-1} *está en* S.

Nótese que estas condiciones reducen el número de condiciones que deben tomarse en cuenta de cuatro a dos. Primero se demostrará que si se cumplen estas condiciones, el conjunto S forma un grupo. Las condiciones (1) y (2) aseguran la cerradura del conjunto, la presencia de la identidad en S y la presencia del inverso de cada elemento a de S en S. Se cumple la ley asociativa puesto que los elementos de S están en G. De aquí que se satisfacen los postulados para un grupo. Por otra parte, si el conjunto S forma un grupo se cumple (1). Ahora, la identidad de G es una identidad para S. Puesto que S es un grupo, su identidad es única y de aquí que la identidad de S es la identidad de G. Además, ya que el inverso de un elemento en G es único, el inverso de un elemento a en S también es el inverso de a en G. Por lo tanto, se cumple (2).

Corolario. Un subconjunto S *de un grupo finito* G *es un subgrupo de* G *si y solamente si* a *y* b *en* S *implica* ab *en* S.

De acuerdo con el teorema, la condición es necesaria. Inversamente, si la condición se satisface, se cumple (1) del teorema. Además, puesto que G es finito, no todas las potencias $a, a^2, a^3, \cdots$ de a en S son distintas, es decir, $a^s = a^t$ para alguna $s > t$. Entonces $a^{s-t} = i$, la identidad de G. De aquí que $a^{s-t-1}a = i$ y a^{s-t-1} en S es el inverso de a. De aquí que se satisface (2) del teorema y S es un subgrupo de G.

Ahora, determinaremos los subgrupos de un grupo cíclico.

Teorema 14. Un subgrupo S *de un grupo cíclico* G *es cíclico. Si* a *es un generador de* G, S *se genera por* a^m, *donde* m *es el menor entero positivo tal que* a^m *esté en* S. *Si* G *es de orden cero, el entero* m *es arbitrario y* S *es isomorfo para el grupo aditivo de múltiplos enteros de* m. *Si* G *es de orden* $n > 0$, m *y* S *es de orden* n/m.

Sea a un generador de G y sea S un subgrupo propio de G. Puesto que S es un subgrupo propio de G, contiene algún elemento a^s y, por lo tanto, también al inverso, a^{-s}, de a^s. Ahora, ya sea s ó $-s$ es un entero positivo. De aquí que m sea el menor entero positivo tal que a^m esté en S. Si a^t está en S, escribir $t = mq + r$, con $0 \leq r < m$. Ahora, $(a^m)^q = a^{mq}$ está en S y, por lo tanto, $a^t a^{-mq} = a^{t-mq} = a^r$ está en S. Sin embargo, $r < m$. De aquí que $r = 0$, por definición de m, y, así, todos los elementos en S son de la forma a^{km}. Por lo tanto, a^m es un generador de S. Si a es de orden cero, a^m es un generador de un subgrupo para todo entero m, y la correspondencia $a^m \leftrightarrow m$ es un isomorfismo entre S y el grupo aditivo de múltiplos enteros de m. Si a es de orden $n > 0$, entonces $a^n = i$ está en S y de aquí que $n = mk$. Por lo tanto, a^m es de orden $k = n/m$.

Ejercicios

1. Seleccionar subgrupos cíclicos de tres órdenes diferentes a partir del grupo simétrico de cuatro símbolos.
2. Exhibir los subgrupos propios en el grupo multiplicativo de las raíces sextas de la unidad.
3. Exhibir los subgrupos propios del grupo aditivo de las clases de residuos módulo 12.
4. Establecer un isomorfismo entre el grupo aditivo de las clases de residuos módulo 12 y el grupo multiplicativo de las raíces decimosegundas de la unidad. ¿Qué raíces de la unidad corresponden a los subgrupos que encontró en el ejercicio 3?
5. Encontrar los elementos del grupo aditivo de las clases de residuos módulo m que pueden usarse como generadores del grupo.
6. Probar que los elementos comunes a dos subgrupos S y T de un grupo G forman un subgrupo de G. Este grupo consiste de los elementos comunes a S y a T y se llama *intersección* de S y T.
7. Demostrar que las permutaciones siguientes forman un grupo:

$i = (1)(2)(3)(4)(5)(6)(7)(8)$, $(1234)(5678)$, $(13)(24)(57)(68)$, $(1432)(5876)$, $(1537)(2846)$, $(1735)(2648)$, $(1836)(2745)$, $(1638)(2547)$. Encontrar tres subgrupos cíclicos de orden 4 de este grupo.
8. Demostrar que los elementos x en un grupo G, tales que $xa = ax$ para todo a en G, forman un subgrupo de G. Este subgrupo se llama *centro* de G.

8 · CLASES LATERALES Y SUBGRUPOS

A continuación, consideraremos algunas propiedades de los grupos que nos darán un conocimiento más amplio de la estructura de un grupo.

DEFINICIÓN. Sea S un subgrupo de G y a un elemento cualquiera de G. La colección de elementos Sa de G que consiste de los productos de cada elemento s de S por el elemento a de G, se llama *clase lateral derecha* de S en G. En forma semejante, la colección de elementos aS de G, se llama *clase lateral izquierda* de S en G.

Nótese que, de acuerdo con esta definición, S es una clase lateral izquierda así como una clase lateral derecha de S en G, porque $iS = Si = S$. También es de interés puntualizar que en un grupo abeliano coinciden las clases laterales derechas y las clases laterales izquierdas de un subgrupo S y que, en este caso, se omiten los adjetivos calificativos derecha e izquierda.

EJEMPLO 1. Sea G el grupo *óctuple* de permutaciones cuyos elementos son $i = (1)(2)(3)(4)$, $a = (1234)$, $b = (13)(24)$, $c = (1432)$, $d = (13)$, $e = (24)$, $f = (12)(24)$, $g = (14)(23)$ y sea S el subgrupo cuyos elementos son i y $d = (13)$. Entonces las clases laterales derechas de S en G son S, Sa, Sc, Se, que consisten, respectivamente, de los conjuntos de los elementos siguientes: $i, (13)$; (1234), Entonces las clases laterales derechas de S en G son S, Sa, Sc, Se, que consisten, respectivamente, de los conjuntos de elementos siguientes: $i, (13)$; $(1234), (14)(23)$; $(1432), (12)(34)$; $(24), (13)(24)$. Nótese que $S = Sd$, $Sa = Sg$, $Sc = Sf$ y $Se = Sb$. Por lo tanto, si se tienen dos clases laterales iguales Sx y Sy, no se concluye que $x = y$, sino solamente que para cada elemento s de S existe un elemento s' de S tal que $sx = s'y$.

EJEMPLO 2. Sea G el grupo aditivo de los enteros y S el subgrupo de los múltiplos enteros de 3. En este caso, las clases laterales de S son los conjuntos de enteros siguientes: $3m, 3m + 1, 3m + 2$. Aquí, puesto que usamos una notación aditiva para G, se escribe $S + a$ en lugar de Sa para una clase lateral derecha de S. Decir que las clases laterales de S son los conjuntos de enteros $3m$, $3m + 1$ y $3m + 2$, simplemente es aseverar que, si sumamos un entero a un múltiplo entero de 3, el resultado es otro múltiplo de 3, un número igual a 1 más un múltiplo de 3, ó un número igual a 2 más un múltiplo de 3.

Los lemas y teoremas siguientes se probarán para las clases laterales derechas, pero debe hacerse notar que pueden establecerse y demostrarse afirmaciones semejantes para las clases laterales izquierdas.

Lema 1. El conjunto de elementos Ss, *donde* s *es cualquier elemento del subgrupo* S, *es el subgrupo* S.

Se escribe $Ss = S$, dando a entender que la colección de elementos Ss es idéntica, excepto en el orden, a los elementos de S. Los elementos del conjunto Ss están en S y todo elemento s' en S está en Ss, puesto que $s' = (s's^{-1})s$ donde $s's^{-1}$ está en S.

Lema 2. Puede establecerse una correspondencia biunívoca entre los elementos de un subgrupo S *y los elementos de una clase lateral derecha* Sa *de* S *en un grupo* G.

La correspondencia $s \leftrightarrow sa$ es biunívoca puesto que $sa = s'a$ implica $s = s'$.

Lema 3. Dos clases laterales derechas Sa *y* Sb *de un subgrupo* S *en un grupo* G, *son idénticas o no tienen elementos comunes.*

Sea x un elemento común a Sa y Sb; esto es, $x = sa = sb$. Entonces, $S(sa) = S(s'b)$. Sin embargo, $S(sa) = (Ss)a = Sa$, de acuerdo con el Lema 1 y, en forma semejante, $S(s'b) = Sb$.

Nótese cómo el ejemplo 1 ilustra el lema 3: $Si \equiv Sd$, $Sa \equiv Sg$, $Sc \equiv Sf$ y $Se \equiv Sb$. Por otra parte, S no tiene elementos en común con Sa, Sc o Se; Sa no tiene elementos en común con S, Sc o Se, etc.

Teorema 15. Los elementos de un grupo G *pueden separarse en clases laterales derechas mutuamente exclusivas de un subgrupo* S *en* G.

Todo elemento a de G pertenece a alguna clase lateral derecha de S en G, a saber, la clase lateral derecha Sa, porque esta clase lateral contiene al elemento $ia = a$. De acuerdo con el lema 3, un elemento dado puede pertenecer a una y solamente a una clase lateral derecha de S. Por lo tanto, se han separado los elementos de G en clases laterales derechas mutuamente exclusivas de S. Frecuentemente se dice de a que es el *representativo* de la clase lateral derecha Sa.

Obsérvese que, en realidad, se ha introducido una relación de equivalencia entre los elementos de un grupo mediante la introducción de las clases laterales derechas. Por supuesto que, se dice que dos elementos a y b de G son congruentes, teniendo como módulo de congruencia al subgrupo S, si $b = sa$, donde s es un elemento de S y se escribe $a \equiv b \pmod{S}$. Nótese que $a \equiv a$ puesto que $a = ia$. Si $a \equiv b$, entonces $b \equiv a$, porque si $b = sa$ entonces $a = s^{-1}b$. Además, si $a \equiv b$ y $b \equiv c$, entonces $a \equiv c$, puesto que se tiene $b = sa$, $c = s'b$ y de aquí que $c = s'(sa)$ $= s''a$. También es importante hacer notar que, si G es el grupo aditivo de los enteros y si S es el subgrupo de los múltiplos enteros de un entero fijo m, el concepto de la separación de G en clases laterales del subgrupo S es el mismo que el de la separación del conjunto de los enteros en clases de residuos módulo m. Estableciendo que dos enteros a y b son congruentes módulo m es lo mismo que decir que pertenecen a la misma clase de residuos módulo m o a la misma clase lateral del subgrupo S.

Teorema 16. Teorema de Lagrange. El orden de un subgrupo S *de un grupo finito* G *es un divisor del orden de* G.

Sea g el orden de G y sea s el orden de S. Sepárense los elementos de G en clases laterales derechas de S, digamos, k en número. De acuerdo con el lema 2, cada clase lateral derecha contiene el mismo número s de elementos. De aquí que $sk = g$.

Corolario 1. El orden de un elemento de un grupo de orden finito divide al orden del grupo.

La demostración es inmediata cuando se recuerda que todo elemento de un grupo genera un subgrupo cíclico del grupo.

Corolario 2. Todo grupo de orden primo p *es cíclico.*

El orden del subgrupo cíclico generado por un elemento $a \neq i$, debe dividir al primo p y de aquí que debe ser de orden p. Por lo tanto, el grupo consiste de las potencias del elemento a.

Corolario 3. Teorema de Fermat. Si a *es un entero y* p *un primo, entonces* $a^p \equiv a \pmod{p}$.

El grupo multiplicativo de los residuos diferentes de cero módulo p, donde p es un primo, es de orden $p - 1$ y 1 es su identidad. Por lo tanto, para todo entero a no congruente a $0 \pmod{p}$, $a^{p-1} \equiv 1 \pmod{p}$ y de aquí que $a^p \equiv a \pmod{p}$. El teorema es trivialmente verdadero si $a \equiv 0 \pmod{p}$.

Ejercicios

1. Encontrar las clases laterales izquierdas del grupo $i = (1)(2)(3)(4)$, $d = (13)$ del grupo óctuple de permutaciones. ¿Son las mismas las clases laterales izquierdas que las clases laterales derechas, encontradas en el ejemplo 1?
2. Separar los elementos del grupo simétrico de cuatro símbolos en clases laterales derechas y también en clases laterales izquierdas del grupo óctuple de cuatro símbolos.

3. Encontrar todos los subgrupos del grupo óctuple de permutaciones.
4. Encontrar todos los subgrupos del grupo simétrico de tres símbolos.
5. Separar los elementos del grupo simétrico de cuatro símbolos en clases laterales derechas e izquierdas del subgrupo $i = (1)(2)(3)(4)$, $(12)(34)$, $(13)(24)$, $(14)(23)$.
6. Probar que una condición necesaria y suficiente para que dos clases laterales derechas Sa y Sb, de un subgrupo S, en un grupo G, sean idénticas es que ab^{-1} sea un elemento de S.
7. ¿Cuáles son los órdenes posibles de los subgrupos del grupo simétrico de cuatro símbolos? Encontrar ejemplos de tantos subgrupos como sea posible.
8. Probar que el número de clases laterales derechas de un grupo finito es igual al número de clases laterales izquierdas del grupo.

9 · TEOREMA DE CAYLEY

Para mostrar la relación íntima que existe entre los grupos de permutaciones y los grupos finitos, se probará el teorema de Cayley.

Teorema 17. Todo grupo finito de orden n *es isomorfo con un grupo de permutaciones sobre* n *símbolos.*

Considérese

$$S_j = \begin{pmatrix} s_1 & s_2 & \cdots & s_n \\ s_1s_j & s_2s_j & \cdots & s_ns_j \end{pmatrix}$$

para $j = 1, 2, \cdots, n$. Entonces, todo S_j es una permutación de los n símbolos del grupo, ya que todos los elementos en la segunda línea de

$$\begin{pmatrix} s_1 & s_2 & \cdots & s_n \\ s_1s_j & s_2s_j & \cdots & s_ns_j \end{pmatrix}$$

son distintos. Es fácil ver que estas permutaciones forman un grupo que es un subgrupo del grupo simétrico de n símbolos. Ya que, de acuerdo con el corolario del teorema 13, solamente se ha establecido la cerradura. Ahora,

$$S_jS_k = \begin{pmatrix} s_1 & s_2 & \cdots & s_n \\ (s_1s_j)s_k & (s_2s_j)s_k & \cdots & (s_ns_j)s_k \end{pmatrix}$$

y $(s_is_j)s_k = s_i(s_js_k)$, donde $s_js_k = s_m$ es un elemento de G. De aquí que S_jS_k es de la forma

$$S_m = \begin{pmatrix} s_1 & s_2 & \cdots & s_n \\ s_1s_m & s_2s_m & \cdots & s_ns_m \end{pmatrix}$$

y la correspondencia biunívoca $s_j \leftrightarrow S_j$ nos proporciona un isomorfismo. Porque, si $s_js_k = s_m$, entonces

$$s_m = s_js_k \leftrightarrow S_m = S_jS_k = \begin{pmatrix} s_1 & s_2 & \cdots & s_n \\ s_1(s_js_k) & s_2(s_js_k) & \cdots & s_n(s_js_k) \end{pmatrix}$$

Este grupo de permutaciones recibe el nombre de grupo de *permutación regular*. Cada uno de sus elementos, excepto la identidad, desplaza n símbolos.

EJEMPLO. Encontrar un grupo de permutación regular isomorfo con el grupo simétrico de tres símbolos. Nómbrense los elementos del grupo simétrico de tres símbolos, de la manera siguiente: $s_1 = (1)(2)(3)$, $s_2 = (123)$, $s_3 = (132)$, $s_4 = (12)$, $s_5 = (13)$, $s_6 = (23)$. Después puede encontrarse la representación de permutación regular a partir de la tabla de multiplicación siguiente. Nótese que se multiplica cada elemento del grupo de la derecha por el elemento que se encuentra en la primera columna. Se obtiene otro grupo de permutación regular si se multiplica a la izquierda, pero, en ese caso, no se tiene el mismo isomorfismo que se estableció en el teorema.

	s_1	s_2	s_3	s_4	s_5	s_6	Grupo de permutación regular
s_1	s_1	s_2	s_3	s_4	s_5	s_6	$S_1 = (s_1)(s_2)(s_3)(s_4)(s_5)(s_6) = i \leftrightarrow s_1$
s_2	s_2	s_3	s_1	s_5	s_6	s_4	$S_2 = (s_1s_2s_3)(s_4s_5s_6) \leftrightarrow s_2$
s_3	s_3	s_1	s_2	s_6	s_4	s_5	$S_3 = (s_1s_3s_2)(s_4s_6s_5) \leftrightarrow s_3$
s_4	s_4	s_6	s_5	s_1	s_3	s_2	$S_4 = (s_1s_4)(s_2s_6)(s_3s_5) \leftrightarrow s_4$
s_5	s_5	s_4	s_6	s_2	s_1	s_3	$S_5 = (s_1s_5)(s_2s_4)(s_3s_6) \leftrightarrow s_5$
s_6	s_6	s_5	s_4	s_3	s_2	s_1	$S_6 = (s_1s_6)(s_2s_5)(s_3s_4) \leftrightarrow s_6$

Una permutación del grupo de permutación regular, reemplaza cada elemento que se encuentra en la primera línea de la tabla por el elemento que está abajo en cualquier línea dada. El isomorfismo está dado al asociar la permutación regular de la derecha a su elemento correspondiente del grupo de la primera columna.

Ejercicios

Encontrar un grupo de permutación regular isomorfo con cada uno de los grupos siguientes:

1. El grupo cíclico de orden 5.
2. El grupo cíclico de orden 6.
3. El grupo óctuple.

4 Anillos, dominios enteros y campos

1 · ANILLOS

Ahora llevaremos nuestro estudio hacia los sistemas algebraicos que tratan con conjuntos cerrados bajo dos operaciones. Las dos operaciones se llamarán adición y multiplicación, y se usará la notación ordinaria para estas operaciones. Sin embargo, debe tenerse presente que estas operaciones pueden no ser la adición y la multiplicación ordinarias sino operaciones bien definidas que satisfagan los postulados dados. El más sencillo de estos sistemas es el anillo.

DEFINICIÓN. Un conjunto de elementos $a, b, c, \cdots$ forma un *anillo* R respecto de las dos operaciones de adición y multiplicación, si:

1. El conjunto forma un grupo conmutativo respecto de la adición.
2. El conjunto es cerrado respecto de la multiplicación.
3. La ley asociativa $a(bc) = (ab)c$ se cumple para la multiplicación.
4. Se cumplen las leyes distributivas $a(b + c) = ab + ac$ y $(b + c)a = ba + ca$.

Puesto que el anillo es un grupo respecto de la adición, se cumplen todas las propiedades de grupo para la adición. La identidad única del grupo aditivo recibe el nombre de elemento cero del anillo, y se denotará por el símbolo ordinario para el número cero. Por lo tanto, $a + 0 = 0 + a = a$ para todo a en el anillo. Se denotará el inverso aditivo único de un elemento a por $-a$ y se escribirá $a + (-a) = a - a = 0$ y $a + (-b) = a - b$. Nótese que las propiedades del inverso aditivo y el elemento cero, nos proporcionan la ley de cancelación, si $a + b = a + c$, entonces $b = c$; una solución única $x = b - a$ de la ecuación $a + x = b$, y la regla $-(-a) = a$.

También puede probarse que $a \cdot 0 = 0$ puesto que $a \cdot 0 + a \cdot a = a(0 + a) = a \cdot a = 0 + a \cdot a$ y de aquí que, de acuerdo con la ley de cancelación para la adición anterior, $a \cdot 0 = 0$. En forma semejante, aplicando la ley distributiva derecha, puede probarse que $0 \cdot a = 0$. Sin embargo, la proposición inversa de que si $a \cdot b = 0$, uno de los factores debe ser cero, no se cumple necesariamente, como se ilustrará a continuación.

Un anillo en el cual la multiplicación es conmutativa recibe el nombre de anillo *conmutativo*. Principalmente nos dedicaremos a los anillos conmutativos.

EJEMPLOS. El estudiante puede comprobar que los enteros, los enteros pares y las clases de residuos módulo m, todos forman anillos conmutativos respecto de la adición y de la multiplicación. Estos anillos difieren en ciertos aspectos. El anillo de los enteros y el anillo de las clases de residuos tienen elementos identidad para la multiplicación, pero el anillo de los enteros pares no lo tiene. Asimismo, la ley de cancelación para la multiplicación se cumple en el anillo de los enteros y en el anillo de los enteros pares, pero no se cumple en el anillo de clases de residuos módulo m a menos que m sea un número primo. Si $m = ab$ es compuesto, se ve que $ab \equiv 0 \pmod{m}$ pero ni $a \equiv 0$, ni $b \equiv 0 \pmod{m}$. Por otra parte, si $ab \equiv 0 \pmod{p}$, donde p es primo, se tiene que $a \equiv 0 \pmod{p}$ o bien $b \equiv 0 \pmod{p}$.

Divisores de cero

Si $ab = 0$ y $a \neq 0$ y $b \neq 0$, entonces a y b reciben el nombre de divisores propios de cero. Así, se observa que el anillo de clases de residuos módulo m, es un anillo sin divisores propios de cero si y solamente si m es primo.

Elemento unidad

Si un anillo contiene un elemento u tal que $ua = au = a$, para todo a en el anillo, u se llama elemento unidad. Se denotará ya sea por u o por el número 1. Puede probarse que el elemento unidad es único. Puesto que, si u' es un segundo elemento unidad, se tiene $u \cdot u' = u' = u$.

Las propiedades usuales de los inversos aditivos pueden establecerse para los elementos de un anillo. Como una ilustración probaremos que $(-a)(-b) = ab$. Considérese $s = (-a)(-b) + (-a)b + ab$. Se demostrará que $s = (-a)(-b)$ y que $s = ab$. Primero, $s = (-a)(-b) + (-a)b + ab = (-a)(-b) + [(-a) + a]b$, aplicando la ley distributiva derecha a los dos últimos términos. Ya que $[(-a) + a]b = 0 \cdot b = 0$, $s = (-a)(-b) + 0 = (-a)(-b)$. Por otra parte, si se aplica

la ley distributiva izquierda a los dos primeros términos, se tiene $s = (-a)[(-b) + b] + ab = (-a) \cdot 0 + ab = 0 + ab = ab$.

Ejercicios

1. Si los elementos del anillo de clases de residuos módulo 10, se denotan por $0, 1, 2, \cdots, 9$, exhibir -2, -3, $-(3 \cdot 2)$, $3(-2)$ y $(-3)2$.
2. Probar que en un anillo
   a. $-(-a) = a$.
   b. $-(ab) = (-a)b = a(-b)$.
   c. $a(b - c) = ab - ac$.
3. Comprobar que los postulados para un anillo se satisfacen en la definición siguiente de un anillo de números: Un conjunto de números complejos forma un anillo si la suma, la diferencia y el producto de dos números cualesquiera, en el conjunto, están también en el conjunto.

2 · DOMINIOS ENTEROS Y CAMPOS

Los anillos pueden distinguirse en muchas formas. Nos interesaremos particularmente en los anillos conmutativos que sean dominios enteros o campos.

Dominio entero

Un anillo conmutativo de, por lo menos, dos elementos es un dominio entero si contiene un elemento unidad u y no contiene divisores propios de cero.*

Campo

Un dominio entero es un campo si todo elemento $a \neq 0$ tiene un inverso multiplicativo a^{-1}, tal que $a^{-1} \cdot a = u$.

En los ejemplos anteriores se observa que los enteros forman un dominio entero, pero no un campo, que los enteros pares forman un anillo, pero no un dominio entero y que las clases de residuos módulo m forman un campo si y solamente si m es primo. Los números racionales, los números reales y los números complejos, son ejemplos de campos respecto de las operaciones de adición y multiplicación. Se define un *subcampo* como un subconjunto de elementos de un campo que forman asimismo un campo, respecto de las operaciones dadas, obsérvese que los números racionales y los números reales son subcampos del campo de los números complejos.

* Algunos autores no exigen la existencia de un elemento unidad para un dominio entero. Ver, por ejemplo, van der Waerden, *Modern Algebra*, vol. 1, pág. 34, Frederick Ungar Publishing Co., Nueva York, 1949.

Es interesante establecer una segunda definición de campo, la cual fácilmente se demuestra que es equivalente a la primera definición.

Segunda definición de campo

Un conjunto de, por lo menos, dos elementos forma un campo respecto de las dos operaciones de adición y multiplicación, si:

1. Es cerrado respecto de la adición y la multiplicación.
2. Forma un grupo conmutativo respecto de la adición, cuya identidad se llama elemento cero.
3. Sus elementos diferentes de cero forman un grupo conmutativo respecto de la multiplicación, cuya identidad se llama elemento unidad.
4. Se cumplen las leyes distributivas: $a(b + c) = ab + ac$ y $(b + c)a = ba + ca$.

Ejercicios

Determinar si los conjuntos siguientes son anillos respecto de la adición y la multiplicación. Si son anillos, ¿son campos o dominios enteros?

1. Los enteros positivos.
2. Los números de la forma $b\sqrt{2}$, con b racional.
3. Los números de la forma $3m$, con m entero.
4. Las raíces cuartas de la unidad.
5. 0.
6. Los números de la forma $a + b\sqrt{2}$, con a y b enteros.
7. Los números de la forma $a + b\sqrt{2}$, con a y b racionales.
8. Los números de la forma $a + bi$, con a y b enteros.
9. Los números de la forma $a + bi$, con a y b racionales.
10. Las clases de residuos módulo 15.
11. Las clases de residuos módulo 11.
12. El conjunto de números $a + b\sqrt[3]{9}$, con a y b racionales.
13. El conjunto de números $a + b\sqrt[3]{2}$, con a y b racionales.
14. Las parejas de números racionales (a, b) con la igualdad, la adición y la multiplicación, definidas de la manera siguiente: $(a, b) = (c, d)$ si y solamente si $a = c$ y $b = d$; $(a, b) + (c, d) = (a + c, b + d)$; $(a, b) \cdot (c, d) = (ac, bd)$.
15. Probar que en un dominio entero $ax = ay, a \neq 0$, implica que $x = y$.
16. Probar que la ecuación $ax = b$, donde $a \neq 0$, tiene una solución única x en un campo. Por lo tanto, siempre es posible la división en un campo, excepto entre cero.
17. Comprobar que los postulados para un campo se satisfacen en la siguiente definición de un campo numérico: Un conjunto de, por lo menos, dos números complejos, forma un campo si la suma, la diferencia, el producto y el cociente, de dos números cualesquiera, también son números del conjunto. Se excluye la división entre cero.

3 · COCIENTES EN UN CAMPO

En un campo, la solución única $a^{-1}b$, de la ecuación $ax = b$, donde $a \neq 0$, frecuentemente se denota mediante el cociente b/a. Por ejemplo, en el anillo de clase de residuos módulo 5, 2/3 significa $2 \cdot 3^{-1} = 2 \cdot 2 = 4$. Puede probarse que las reglas siguientes gobiernan a los cocientes:

1. $a/b = c/d$ si y solamente si $ad = bc$;
2. $a/b + c/d = (ad + bc)/(bd)$;
3. $(a/b)(c/d) = (ac)/(bd)$.

Ya que estas reglas pueden probarse fácilmente a partir de la definición de cociente, se deja la demostración al estudiante.

Ejercicios

1. Probar las afirmaciones (1), (2) y (3), dadas en el párrafo anterior.
2. En el anillo de clases de residuos módulo 7, representar 1/3, −1/3, −3/5.
3. Probar que en un campo:
   a. $(a/b) - (c/d) = (ad - bc)/bd$;
   b. si $a/b \neq 0$, entonces $(a/b)(b/a) = u$;
   c. $(-a)^{-1} = (a^{-1})$;
   d. $-(a/b) = (-a)/b = a/(-b)$;
   e. $(-a)/(-b) = a/b$.

4 · CAMPO DE COCIENTES

Tal y como se construyeron los números racionales a partir de los enteros, de manera que los números racionales contuvieran un subconjunto isomorfo a los enteros, puede construirse un campo a partir de los elementos de un dominio entero de modo que un subconjunto de los elementos del campo sea isomorfo al dominio entero. Se dice que el dominio entero está *incluido* en el campo. La construcción de este campo, llamado *campo de cocientes* del dominio entero, es muy semejante a la construcción de los números racionales como parejas ordenadas de enteros. Será útil para el estudiante el comparar cada paso en la construcción dada aquí, con el paso correspondiente en la construcción de los números racionales.

Teorema 1. Puede construirse un campo a partir de los elementos de un dominio entero.

Sean $a, b, c, \cdots$ los elementos del dominio entero I. Considérense las parejas ordenadas de elementos (a, b), con $b \neq 0$. Se define la igualdad de dos parejas de la manera siguiente: $(a, b) = (c, d)$ si y solamente si $ad = bc$. Esta igualdad es una relación de equivalencia ya que se ve fácilmente que es simétrica y reflexiva, y se demuestra que es transitiva. Si $(a, b) = (c, d)$ y si $(c, d) = (e, f)$, entonces, $ad = bc$ y $cf = de$. De aquí que $adf = bcf = bde$. Puesto que $d \neq 0$, puede aplicarse la ley de cancelación para la multiplicación (ver el ejercicio 15, página 82 y obtener $af = be$, la condición requerida para la igualdad de (a, b) y (e, f). Por lo tanto, se ve que las parejas (a, b) se separan en clases de parejas iguales. Una clase dada puede representarse por cualquier par de ella.

Sean (a, b) y (c, d) representativos de dos clases cualesquiera. Se definen la suma y el producto de dos clases representadas por (a, b) y (c, d), como las clases cuyos pares representativos se obtienen de la manera siguiente:

$$(a, b) + (c, d) = (ad + bc, bd),$$

$$(a, b) \cdot (c, d) = (ac, bd).$$

El estudiante puede comprobar que se obtienen las mismas clases de suma y producto si se reemplaza (a, b) por una pareja $(a', b') = (a, b)$ y (c, d) se reemplaza por una pareja $(c', d') = (c, d)$.

Falta por probar que estas clases forman un campo respecto de la adición y de la multiplicación. Los detalles de la demostración se dejan al estudiante. Debe comprobarse que se cumplen las leyes asociativa, conmutativa y distributiva; que el elemento cero es $(0, a)$, donde 0 es el cero del dominio entero; que el inverso aditivo de (a, b) es $(-a, b)$; que el elemento unidad es (u, u), donde u es el elemento unidad del dominio entero; y que el inverso multiplicativo de (a, b), donde $a \neq 0$, es (b, a).

Teorema 2. El campo de cocientes de un dominio entero contiene un subconjunto de elementos isomorfo al dominio entero.

Se establece la siguiente correspondencia biunívoca entre los elementos $a, b, c, \cdots$ del dominio entero y las clases con pares representativos $(a, u), (b, u), (c, u), \cdots$ del campo de cocientes. Por lo tanto, si

$$(a, u) \leftrightarrow a \quad \text{y} \quad (b, u) \leftrightarrow b,$$

entonces

$$(a, u) + (b, u) = (au + bu, u^2) = (a + b, u) \leftrightarrow a + b$$

y

$$(a, u) \cdot (b, u) = (ab, u^2) = (ab, u) \leftrightarrow ab,$$

y se establece el isomorfismo.

Si el dominio entero I, ya es un subconjunto de un campo F, entonces el campo de cocientes de I es isomorfo con un subcampo del campo F. Puesto que puede establecerse la correspondencia biunívoca $(a, b) \leftrightarrow a/b = ab^{-1}$, donde a y $b \neq 0$ son elementos del dominio entero. Obsérvese que, en general, b^{-1} no es un elemento del dominio entero. De aquí se ve por qué el campo de cocientes recibió ese nombre. Además, puede probarse que el campo de cocientes es una extensión mínima del dominio entero I hacia un campo, en el sentido de que cualquier campo que contenga I contiene un subcampo isomorfo al campo de cocientes del dominio entero.

EJEMPLOS. Sea F el campo de números reales e I el dominio entero de los enteros. Entonces, el campo de cocientes de I es el campo de los números racionales, un subcampo de F.

Determinar el campo de cocientes del dominio entero de clases de residuos módulo 3. Aquí, las clases del campo de cocientes son:

$$0: (0, 1), (0, 2);$$
$$1: (1, 1), (2, 2);$$
$$2: (2, 1), (1, 2);$$

Se ve que el campo de cocientes es isomorfo con el dominio entero de clases de residuos módulo 3.

Ejercicios

1. Probar que las clases de suma y producto del campo de cocientes, son independientes de los pares particulares (a, b) y (c, d) usados en la definición.
2. Probar que las clases del campo de cocientes de un dominio entero obedecen las leyes asociativa y conmutativa para la adición y la multiplicación, y la ley distributiva.
3. Probar que el inverso multiplicativo de la clase representada por (a, b), donde $a \neq 0$, es la clase representada por (b, a).
4. ¿Cuál es el campo de cocientes del dominio entero de las clases de residuos módulo 5?
5. ¿Cuál es el campo de cocientes del dominio entero de los números complejos $a + bi$, donde a y b son enteros?

5 · POLINOMIOS SOBRE UN DOMINIO ENTERO

Sea x un símbolo arbitrario que es conmutativo con los elementos de un dominio entero I. Para un entero positivo n, sea $x^n = x \cdot x \cdots x$ hasta n *factores*. Además, se define $u \cdot x = x$, donde u es el elemento unidad de I. Un *polinomio*, en el dominio entero I, es una expresión finita de la forma

$$(1) \qquad f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

donde los coeficientes a_i son elementos de I. La potencia de x que multiplica a a_0 es x^0, que se define como igual a u. Si una potencia de x no aparece en $f(x)$ se considera que su coeficiente es cero.

Dos polinomios son iguales si y solamente si los coeficientes de las potencias semejantes de x son iguales; es decir, si y solamente si son idénticos. En esta definición de igualdad los polinomios se consideran como formas, no estamos discutiendo sus valores funcionales. Manténgase en mente que x es un símbolo arbitrario y que hasta el momento no se le ha asignado significado. Es un *indeterminado*.

A continuación, definiremos la suma y el producto de dos polinomios. Sea $f(x)$ el polinomio (1) y $g(x)$ el polinomio

$$(2) \qquad g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m,$$

siendo los b_i elementos en I. Entonces

$$(3) \quad f(x) \pm g(x) = (a_0 \pm b_0) + (a_1 \pm b_1)x + \cdots + (a_m \pm b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_nx^n, \quad m < n,$$

y

$$(4) \quad f(x) \cdot g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_mx^{n+m},$$

siendo el coeficiente de x^k

$$a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \cdots + a_kb_0.$$

Si $a_n \neq 0$, entonces n recibe el nombre de *grado* del polinomio $f(x)$. Obsérvese que los polinomios de grado cero son los elementos diferentes

de cero del dominio entero I. El polinomio cero no tiene grado. Obsérvese también que el grado del producto de dos polinomios es la suma $m + n$ de los grados de los factores.

Teorema 3. Los polinomios (1), en un dominio entero I, *con suma y producto definidos por (3) y (4), forman un dominio entero.*

Este dominio entero se denota por $I[x]$. Se deja al estudiante la demostración en detalle. Pueden verificarse las leyes conmutativa, asociativa y distributiva. Es obvio que el elemento cero y el elemento unidad, son el elemento cero y el elemento unidad de dominio entero de coeficientes. No hay divisores propios de cero, puesto que si $f(x)$ y $g(x)$ están dados por (1) y (2), con $a_n \neq 0$ y $b_m \neq 0$, el producto (4) no es cero ya que $a_nb_m = 0$ si y solamente si $a_n = 0$, ó si $b_m = 0$.

Ejercicios

Establecer las propiedades siguientes en $I(x)$:

1. La ley conmutativa para la adición.
2. La ley conmutativa para la multiplicación.
3. La ley asociativa para la adición.
4. La ley asociativa para la multiplicación.
5. Las leyes distributivas izquierda y derecha.

6 · CARACTERISTICAS DE UN DOMINIO ENTERO

Sea u el elemento unidad del dominio entero I. El elemento unidad genera un grupo aditivo cíclico. Si k es un entero positivo, $ku = u + u + \cdots + u$ con k términos. Interpretando aditivamente las definiciones y las leyes de los exponentes, establecidas para las potencias de un elemento de un grupo, se tiene $0 \cdot u = 0$, $(-k)u = k(-u)$, $ru + su = (r + s)u$ y $s(ru) = (sr)u = r(su)$. Ahora, tal y como se ha visto, un grupo cíclico es isomorfo al grupo aditivo de enteros o al grupo aditivo de clases de residuos módulo m. En el último caso se probará que m es primo.

Teorema 4. Si el grupo aditivo cíclico generado por u, *el elemento unidad de un dominio entero, es de orden* m > 0, m *es un primo* p.

Sea $m = rs$. Entonces $(ru)(su) = (\underbrace{u + u + \cdots + u}_{r\ \text{términos}})(\underbrace{u + u + \cdots + u}_{s\ \text{términos}}) = \underbrace{u^2 + u^2 + \cdots + u^2}_{rs\ \text{términos}} = (rs)u^2 = (rs)u = 0$. Pero ru y su son

elementos del dominio entero, que no tiene divisores propios de cero. De aquí que $ru = 0$, o bien $su = 0$, lo que contradice la suposición de que el grupo cíclico generado por u tiene orden m. Por lo tanto, m es un primo p.

DEFINICIÓN. El orden del grupo aditivo cíclico generado por el elemento unidad u de un dominio entero se llama *característica* del dominio entero. Por lo tanto, la característica es un primo positivo p o cero.

Teorema 5. Un dominio entero cuya característica es cero, contiene un subconjunto de elementos que es isomorfo al dominio entero de los enteros, y un dominio entero cuya característica es un primo p, *contiene un subconjunto de elementos que es isomorfo al campo de clases de residuos módulo* p.

Si el grupo cíclico generado por u es de orden cero, entonces los elementos ku son distintos y la correspondencia biunívoca $ku \leftrightarrow k$ es un isomorfismo, porque si $ru \leftrightarrow r$ y $su \leftrightarrow s$, entonces $ru + su = (r+s)u \leftrightarrow r + s$ y $(ru)(su) = (rs)u \leftrightarrow rs$. Si el grupo cíclico generado por u es de orden primo p, los elementos ku para los cuales k pertenece a la misma clase de residuos módulo p son iguales y la correspondencia $ku \leftrightarrow C_k$, donde C_k denota la clase de residuos que contiene el entero k, nos proporciona un isomorfismo entre los elementos ku y las clases de residuos módulo p.

Teorema 6. En un dominio entero todos los elementos diferentes de cero generan grupos aditivos cíclicos del mismo orden.

Sean u el elemento unidad y a cualquier elemento diferente de cero del dominio entero. Para un dominio entero de característica p, se comprueba fácilmente que $pa = p(au) = p(ua) = (pu)a = 0$. Además, si $ma = 0$, donde $a \neq 0$ y $m \neq 0$, entonces $ma = m(ua) = (mu)a = 0$ y de aquí que $mu = 0$, dándonos $m = kp$; es decir, p es el menor entero m tal que $ma = 0$. Para un dominio entero de característica cero, $ma \neq 0$ si $a \neq 0$ y $m \neq 0$, porque, en la misma forma, $ma = (mu)a$ y $mu \neq 0$ si $m \neq 0$. (Nótese que aquí se está aplicando el símbolo 0 en dos formas diferentes. Cuando se escribe $a \neq 0$, se da a entender que a no es la identidad aditiva del dominio entero bajo consideración. Pero cuando se escribe $m \neq 0$, se da a entender que m no es la identidad aditiva para los enteros).

Puesto que los campos son dominios enteros, pueden separarse también en dos tipos esencialmente diferentes, campos cuya característica

es un primo p y campos de característica cero. El campo de cocientes del dominio entero de múltiplos enteros del elemento unidad u es, en el caso de característica p, isomorfo al campo de clases de residuos módulo p, y en el caso de característica cero, isomorfo al campo de números racionales. Por lo tanto, un campo contiene un subcampo que es isomorfo al campo de clases de residuos módulo p o al campo de números racionales.

7 · DIVISION EN UN DOMINIO ENTERO

A continuación, haremos una lista de algunas definiciones que se aplican en cualquier dominio entero y veremos que son semejantes a las correspondientes definiciones dadas cuando se estudiaron las propiedades de divisibilidad de los enteros.

Divisor

Un elemento b, en un dominio entero I, es un divisor de un elemento a en I, si existe en I un elemento c tal que $a = bc$.

Asociados y unitarios

Dos elementos diferentes de cero, a y b, en un dominio entero I son asociados, si a divide a b y b divide a a. Un unitario es un asociado del elemento unidad de I.

Teorema 7. Un elemento a, *en un dominio entero* I, *es un unitario en* I *si y solamente si tiene un inverso multiplicativo en* I; *es decir, aquellos y solamente aquellos elementos en* I *que tienen inversos multiplicativos en* I *son unitarios.*

Ahora, si a es un unitario divide a u, el elemento unidad de I, y se tiene $ab = u$. Por tanto, b es un inverso multiplicativo de a. Por otra parte, si a tiene un inverso multiplicativo b, $ab = u$ y a divide a u. El elemento unidad u divide a cualquier elemento a en I puesto que $au = a$. De aquí que a es unitario.

Teorema 8. Dos elementos en I *son asociados si y solamente si uno es unitario multiplicado por el otro.*

Sean a y b asociados en I. Entonces, $a = bc$ y $b = ad$. De donde $a = adc$. Pero también, $a = au$ y de aquí que $au = adc$. Aplicando la

ley de cancelación para la multiplicación, se tiene $u = dc$ lo que implica que c y d son unitarios. Por lo tanto, si dos elementos son asociados, uno es un unitario multiplicado por el otro. Por otra parte, si $b = au'$, donde u' es un unitario tal que $u'u'' = u$, entonces b divide a a, puesto que $a = au = a(u'u'') = (au')u'' = bu''$. Puesto que $b = au'$, a divide a b y de aquí que a y b son asociados si uno es un unitario multiplicado por el otro.

Corolario. Cualquier elemento a *en* I *es divisible entre los unitarios de* I.

Puesto que si u' es un unitario tal que $u'u'' = u$, se tiene $a = au = a(u'u'') = (au'')u'$ y de aquí que u' divide a a.

Divisores propios e impropios

Todo elemento a diferente de cero de un dominio entero es divisible entre sus asociados (por definición) y entre los unitarios del dominio entero (de acuerdo con el corolario del teorema 8). Estos divisores de a se llaman divisores impropios de a. Todos los demás divisores reciben el nombre de divisores propios.

Primo o elemento irreducible

Un elemento a diferente de cero de un dominio entero que no es unitario y que no tiene divisores propios se llama primo o elemento irreducible. Si un elemento tiene divisores propios es *reducible.*

EJEMPLOS. Puesto que todo elemento diferente de cero en un campo tiene un inverso multiplicativo, los unitarios de un campo son sus elementos diferentes de cero.

En el dominio polinomial $I[x]$ los unitarios son los unitarios del dominio entero I de los coeficientes. Para probar este hecho, sea $f(x) \cdot g(x) = u$, el elemento unidad de I. Ya que el grado del producto de dos polinomios es la suma de los grados de los factores, tanto $f(x)$ como $g(x)$ deben ser polinomios de grado cero.

En el dominio polinomial $F[x]$, donde F es un campo, los asociados del polinomio $f(x)$ son $cf(x)$, donde c es cualquier elemento diferente de cero del campo.

En el dominio entero de los enteros, los enteros primos son los elementos irreducibles.

El polinomio $x^2 - 2$ es irreducible en el campo de los números racionales, pero, puesto que $(x - \sqrt{2})(x + \sqrt{2}) = x^2 - 2$, el polinomio $x^2 - 2$ es reducible en el campo de los números reales. Obsérvese que, en consecuencia, esa irreducibilidad es una propiedad que depende del dominio entero que se considere en particular.

Para ilustrar un poco más las definiciones anteriores, considérese el dominio entero I cuyos elementos son de la forma $a + b\sqrt{13}$, donde a y b son

enteros. Se deja al estudiante la realización de las demostraciones que se omiten en las afirmaciones siguientes. Sea $\alpha = a + b\sqrt{13}$. Definimos $N(\alpha) = (a + b\sqrt{13})(a - b\sqrt{13}) = a^2 - 13b^2$, del cual se observa que es entero. $N(\alpha)$ recibe el nombre de *norma* de α.

1. Probar que $N(\alpha\beta) = N(\alpha)N(\beta)$.
2. El elemento α es unitario si y solamente si $N(\alpha) = \pm 1$.

Si $N(\alpha)$ ± 1, *entonces* α es unitario porque $(a + b\sqrt{13})(a - b\sqrt{13}) = \pm 1$ y $a + b\sqrt{13}$ divide al elemento unidad 1. Si α es unitario, se tiene $\alpha\beta = 1$ y de aquí que $N(\alpha\beta) = N(\alpha)N(\beta) = 1$. Como $N(\alpha)$ y $N(\beta)$ son enteros, $N(\alpha) = \pm 1$ y $N(\beta) = \pm 1$.

3. $18 - 5\sqrt{13}$ y $-18 - 5\sqrt{13}$ son unitarios.
4. $1 + \sqrt{13} = (-18 - 5\sqrt{13})(-47 + 13\sqrt{13})$ y $-47 + 13\sqrt{13} = (18 - 5\sqrt{13})(1 + \sqrt{13})$ son asociados pero no unitarios.
5. $2, -3 - \sqrt{13}$ y $3 - \sqrt{13}$ son primos de I. Puesto que, supóngase que $\alpha\beta = 2$; entonces, $N(\alpha\beta) = N(\alpha)N(\beta) = 4$, de modo que $N(\alpha) = \pm 2$ ó ± 4, ó $N(\beta) = 2$ ó ± 4. Supóngase que $N(\alpha) = \pm 4$; entonces, $N(\beta) = \pm 1$ y β es unitario. En forma semejante, si $N(\beta) = \pm 4$, α es unitario, y ahora supóngase que $N(\alpha) = \pm 2 = a^2 - 13b^2$ donde $\alpha = a + b\sqrt{13}$. Entonces $a^2 \equiv \pm 2 \pmod{13}$. Fácilmente se ve, probando las posibilidades $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5$ y ± 6 para a, que esta congruencia no tiene solución. De aquí que, si $\alpha\beta = 2$, α ó β es unitario, así que 2 es primo en I. En forma semejante, si $\alpha\beta = -3 - \sqrt{13}$ ó $3 - \sqrt{13}$, se tiene $N(\alpha)N(\beta) = -4$ y siguiendo los mismos pasos puede demostrarse que α ó β es unitario.
6. Obsérvese que $4 = 2 \cdot 2 = (-3 - \sqrt{13})(3 - \sqrt{13})$ y de aquí que la factorización única en elementos irreducibles o primos no se cumple en I.

Los conceptos de divisibilidad, discutidos en esta sección, se aplicarán en el siguiente capítulo al dominio entero particular de polinomios en un campo.

Ejercicios

1. En el dominio entero $F[x]$, donde F es el campo de los números racionales, ¿es el polinomio $2x^3 - 2$ un divisor de $x^3 - 1$?; ¿es $2x^3 - 2$ divisible entre el polinomio 3? Si la respuesta es sí, exhibir la factorización.
2. ¿Cuáles son los unitarios del dominio entero de las clases de residuos módulo 5?
3. ¿Cuáles son los unitarios del dominio entero de los números complejos de la forma $a + bi$, donde a y b son racionales?
4. ¿Son unitarios $1, -1, i, -i$, en el dominio entero de los números complejos de la forma $a + bi$, donde a y b son enteros?

8 · DOMINIOS ENTEROS ORDENADOS

Los enteros se dividen en tres clases: los enteros positivos, los enteros negativos y cero. A continuación, generalizaremos este concepto para un dominio entero arbitrario.

DEFINICIÓN. Se dice que un dominio entero I es *ordenado*, si existe un subconjunto P de elementos de I tales que para todo elemento a de I se cumple una y solamente una de las siguientes alternativas: (1) a está en P; (2) $-a$ está en I; ó (3) $a = 0$, y, si x está en P y y está en P, también lo están $x + y$ y xy. El conjunto P recibe el nombre de conjunto de *elementos positivos* de I.

EJEMPLOS. Los enteros, los números racionales y los números reales, todos son dominios enteros ordenados bajo la definición usual de número positivo.

Los números complejos no forman un dominio entero ordenado. Para demostrarlo, primero se probará un teorema.

Teorema 9. Si 1 *es la identidad multiplicativa de un dominio entero ordenado* I, *entonces* 1 *es un elemento positivo de* I.

Ahora, $1 \neq 0$ y, si 1 no está en P, -1 está en P. Pero entonces, $(-1)(-1) = 1$ está en P, una contradicción.

A continuación, considérese el número complejo i. Puesto que $i \neq 0$, i está en P o sea $-i$ está en P. Pero si i está en P, $i \cdot i = -1$ está en P, lo que contradice al teorema 9. De aquí que $-i$ está en P. Pero, una vez más, entonces se tiene $(-i)(-i) = -1$ en P y de aquí que los números complejos no pueden ser ordenados.

Pueden definirse las desigualdades en cualquier dominio entero ordenado: $a > b$ si y solamente si $a - b$ está en P. En particular, $a > 0$ si y solamente si $a - 0 = a$ está en P. De modo semejante, se dice que $a < b$ si y solamente si $b - a$ está en P. A partir de estas definiciones pueden extenderse los resultados de la Sec. 9, Cap. 1, para cualquier dominio entero ordenado.

Todo campo es también un dominio entero y es natural que se defina un *campo ordenado* como un campo para el cual, cuando se considera como un dominio entero, es un dominio entero ordenado. Por otra parte, supóngase que se tiene un dominio entero ordenado I que no es un campo y se forma el campo de cocientes F de I. Recuérdese que el campo de cocientes consiste de clases de pares (a, b) con a y b elementos de I. Además, se ha demostrado que la identidad aditiva de F es la clase de pares de la forma $(0, a)$ y que I es isomorfo al conjunto de clases con representativos $(a, 1)$. Debido a este isomorfismo y al hecho de que una clase dada puede representarse por cualquiera de las parejas que contiene, puede considerarse que todo elemento de I es un elemento de F. Ahora se dirá que una ordenación de I *se extiende* a una ordenación de F, si un elemento a de I es un elemento positivo de I si y solamente si es un elemento positivo de F.

Teorema 10. Sea I *un dominio entero ordenado y* F *el campo de cocientes de* I. *Entonces, la ordenación de* I *puede extenderse a una ordenación de* F *en una y solamente en una forma. Específicamente, si* (a, b) *es un representativo de uno de los elementos de* F, *entonces* (a, b) *es un elemento positivo de* F *si y solamente si* ab *es un elemento positivo de* I.

En todo dominio entero ordenado el cuadrado de cualquier elemento diferente de cero es positivo, puesto que $a^2 = (-a)^2$ y a es positivo ó $-a$ es positivo. De aquí que, si (a, b) $(b \neq 0)$ es un elemento positivo de F, también lo es $(a, b)(b, 1)^2 = (ab, 1)$. Por lo tanto, si (a, b) es un elemento positivo de F, ab es un elemento positivo de I.

Por otra parte, supóngase que se define (a, b) como un elemento positivo de F si y solamente si ab es un elemento positivo de I. Ahora, si $(a, b) \neq (0, 1)$, $ab \neq 0$ y de aquí que $ab > 0$ ó $ab < 0$. Si $ab < 0$, $-(ab) = (-a)b > 0$. De aquí que (a, b) es cero, (a, b) es positivo ó $-(a, b) = (-a, b)$ es positivo, y solamente se cumple una de estas alternativas. Si (a, b) y (c, d) son elementos positivos de F, entonces $(a, b)(c, d) = (ac, bd)$ es un elemento positivo de F, puesto que $(ac)(bd) = (ab)(cd)$ es un elemento positivo de I. Finalmente, si (a, b) y (c, d) son elementos positivos de F, entonces $(a, b) + (c, d) = (ad + bc, bd)$ es un elemento positivo de F, puesto que $(ad + bc)(cd) = (ab)d^2 + (cd)b^2$ es un elemento positivo de I. De aquí que F es un campo ordenado.

Ejercicios

1. Probar que en todo campo ordenado:
   a. $0 < 1/a$ si y solamente si $a > 0$.
   b. $0 < a < b$ implica que $0 < 1/b < 1/a$.
   c. $a < b < 0$ implica que $0 > 1/a > 1/b$.
   d. $a_1^2 + a_2^2 + \cdots + a_n^2 \geq 0$.

2. Demostrar que:
   a. En todo campo, $a/b + a/c = a/(b + c)$ implica que $a = 0$ ó $b^2 + bc + c^2 = 0$.
   b. En un campo ordenado, eso implica que $a = 0$.

5 Polinomios sobre un campo

1 · ALGORITMO DE LA DIVISION

Ahora se establecerán las propiedades de divisibilidad de los polinomios sobre un campo que son análogas a las propiedades de divisibilidad de los enteros.

Teorema 1. Algoritmo de la división. Si $g(x) \neq 0$ *y* $f(x)$ *son dos polinomios cualesquiera sobre un campo* F, *existen los polinomios únicos* $q(x)$ *y* $r(x)$ *en* F *tales que*

$$f(x) = g(x) \cdot q(x) + r(x),$$

donde $r(x)$ *puede ser cero o de un grado menor que el grado de* $g(x)$.

Sea

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

y

$$g(x) = b_0 + b_1x + \cdots + b_mx^m, \quad b_m \neq 0.$$

Si $f(x)$ es cero o si el grado de $f(x)$ es menor que el grado m de $g(x)$, se tiene la representación

$$f(x) = 0 \cdot g(x) + f(x).$$

Por tanto, sea $n \geq m$. Entonces, fórmese la diferencia

$$(1) \qquad f(x) - \frac{a_n}{b_m}x^{n-m}g(x) = f_1(x).$$

Ahora, $f_1(x)$ es un polinomio sobre F de grado menor que n. Se realiza la demostración por inducción. Supóngase que el algoritmo es cierto para todos los polinomios sobre F de grado menor que n. Puesto que $f_1(x)$ es ese polinomio, puede escribirse

$$f_1(x) = q_1(x) \cdot g(x) + r(x), \tag{2}$$

donde $r(x)$ es cero o de grado menor que el grado de $g(x)$. Entonces, puede escribirse (1) con la ayuda de (2) como

$$f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = q_1(x) \cdot g(x) + r(x),$$

y de aquí que

$$\begin{aligned} f(x) &= \left[\frac{a_n}{b_m} x^{n-m} + q_1(x)\right] \cdot g(x) + r(x) \\ &= q(x) \cdot g(x) + r(x), \end{aligned}$$

y se tiene la representación deseada de $f(x)$.

Falta por demostrar que los polinomios $q(x)$ y $r(x)$ son únicos. Supóngase que existe un segundo par de polinomios $q'(x)$ y $r'(x)$ tales que

$$f(x) = q'(x) \cdot g(x) + r'(x),$$

donde $r'(x)$ es cero o de grado menor que el grado de $g(x)$. De aquí que

$$q'(x) \cdot g(x) + r'(x) = q(x) \cdot g(x) + r(x)$$

y

$$g(x)[q'(x) - q(x)] = r(x) - r'(x).$$

Ahora, el segundo miembro de esta ecuación es cero o de grado menor que el grado de $g(x)$. Por lo tanto, a menos que $q'(x) - q(x) = 0$, se tiene una contradicción. En consecuencia, $q'(x) = q(x)$ y $r(x) = r'(x)$.

El polinomio $q(x)$ se llama *cociente* y el polinomio $r(x)$ recibe el nombre de *residuo* en el algoritmo de la división.

Corolario 1. Teorema del residuo. Cuando un polinomio f(x) *se divide entre* x − a, *el residuo es* f(a).

Este hecho es inmediato a partir del algoritmo de la división, porque cuando se sustituye $g(x)$ por $x - a$, el resto se transforma en r, un elemento en el campo, y se tiene $f(a) = (a - a) \cdot q(a) + r = r$. Por lo tanto, $f(x) = (x - a) \cdot q(x) + f(a)$. A partir de esta última fórmula se ve inmediatamente que $f(x)$ tiene el factor $x - a$ si y solamente si $f(a) = 0$. De aquí se tiene el siguiente corolario.

Corolario 2. Teorema del factor. Un polinomio f(x) *es divisible entre* x − a *si y solamente si* f(a) = 0.

DEFINICIÓN. Un elemento a recibe el nombre de *cero* de un polinomio $f(x)$ si $f(a) = 0$.

2 · DIVISION SINTETICA

Para encontrar con mayor facilidad el cociente $q(x)$ y el residuo r, cuando se divide un polinomio $f(x)$ sobre un campo F entre el polinomio $x - c$ en F, se introduce el método de la división sintética. Sea

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n$$

y

$$q(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1},$$

entonces

$$\begin{aligned} f(x) &= (x - c)q(x) + r \\ &= (r - cb_0) + (b_0 - cb_1)x + (b_1 - cb_2)x^2 + \cdots \\ &\quad + (b_{n-2} - cb_{n-1})x^{n-1} + b_{n-1}x^n. \end{aligned}$$

Igualando los coeficientes de $f(x)$ cuando se expresa en estas dos formas, se tiene

$$a_n = b_{n-1},\ a_{n-1} = b_{n-2} - cb_{n-1}, \cdots, a_1 = b_0 - cb_1,\ a_0 = r - cb_0.$$

Para realizar los cálculos puede arreglarse el trabajo de la siguiente manera:

a_n	a_{n-1}	$\cdots$	a_1	a_0	$\lfloor c$
	cb_{n-1}	$\cdots$	cb_1	cb_0	
$b_{n-1} = a_n$	$b_{n-2} = a_{n-1} + cb_{n-1}$	$\cdots$	$b_0 = a_1 + cb_1$	$r = a_0 + cb_0$	

Por lo tanto, enlistando simplemente los coeficientes y realizando multiplicaciones y adiciones sencillas, puede leerse el cociente y el residuo directamente en la última línea.

EJEMPLO. Encontrar el cociente y el residuo cuando se divide el polinomio $3x^3 - 4x + 2$ entre $x + 3$. Aplicando la división sintética, se tiene

$$\begin{array}{rrrr|l} 3 & 0 & -4 & 2 & \underline{-3} \\ & -9 & 27 & -69 & \\ \hline 3 & -9 & 23 & -67, & \end{array}$$

la cual proporciona $3x^2 - 9x + 23$ como cociente y -67 como residuo.

Ejercicios

1. Encontrar el cociente y el residuo cuando:
   a. Se divide $-x^4 + 7x^3 + 10x^2 - 5$ entre $x - 2$;
   b. Se divide $3x^3 + 6x^2 - 3x$ entre $x + 1$;
   c. Se divide $x^3 + i$ entre $x - i$.
2. Si $f(x) = 2x^3 + 3x^2 - 1$, encontrar $f(2)$, $f(-3)$, $f(i)$.
3. En el campo de las clases de residuos módulo 5, exhibir el cociente y el residuo cuando se divide el polinomio $3x^3 + 4x^2 + 2x - 2$ entre $2x^2 + 1$.
4. Determinar si los siguientes polinomios son reducibles o irreducibles sobre el campo de las clases de residuos módulo 5. ¿Sobre el campo de las clases de residuos módulo 7?
   a. $x^2 - x + 3$.
   b. $x^3 + 3x^2 + x - 4$.

3 · MAXIMO COMUN DIVISOR

Polinomio mónico

Un polinomio recibe el nombre de mónico * si el coeficiente de la mayor potencia de x es el elemento unidad del campo.

Máximo común divisor

Un polinomio $d(x)$ es un máximo común divisor de dos polinomios $f(x)$ y $g(x)$ si $d(x)$ divide a $f(x)$ y $g(x)$ y si $a(x)$ es un divisor común de $f(x)$ y $g(x)$, entonces $a(x)$ divide a $d(x)$. Obsérvese que, si existe un máximo común divisor $d(x)$, entonces todo asociado de $d(x)$ también es un máximo común divisor de $f(x)$ y $g(x)$. Frecuentemente se dice que ese asociado de $d(x)$ que sea mónico es el máximo común divisor de $f(x)$ y $g(x)$.

Teorema 2. Algoritmo Euclideano. Dos polinomios $f(x)$ *y* $g(x)$ *diferentes de cero sobre un campo F, tienen un máximo común divisor* $d(x)$ *sobre F.*

* Se usa este término como traducción del vocablo inglés *monic*. (N. del T.)

La demostración es la misma que la demostración para la construcción del máximo común divisor de dos enteros diferentes de cero. Se aplica el algoritmo de la división a $f(x)$ y $g(x)$, obteniendo

$$(3) \qquad f(x) = g(x) \cdot q(x) + r(x),$$

donde $r(x)$ es cero o de grado menor que el grado de $g(x)$. Si $r(x)$ es cero, entonces un máximo común divisor de $f(x)$ y $g(x)$ es el propio $g(x)$. Si $r(x) \neq 0$, se probará que un máximo común divisor de $f(x)$ y $g(x)$ es un máximo común divisor de $g(x)$ y $r(x)$, reduciéndose en esta forma el problema de encontrar un m.c.d. de $f(x)$ y $g(x)$ al encontrar un m.c.d. de $g(x)$ y $r(x)$. Sea $d(x)$ un máximo común divisor de $f(x)$ y $g(x)$ y sea $d'(x)$ un máximo común divisor de $g(x)$ y $r(x)$. Puesto que $d'(x)$ divide a $g(x)$ y $r(x)$, de acuerdo con (3) se ve que divide a $f(x)$, y de aquí que es un divisor común de $f(x)$ y $g(x)$. Por lo tanto, $d'(x)$ divide a $d(x)$. En forma semejante, (3) demuestra que $d(x)$ divide a $r(x)$ y, por lo tanto, $d'(x)$ es divisible entre $d(x)$. De aquí que $d(x)$ y $d'(x)$ son asociados y solamente difieren en un factor que es un elemento de F.

Ahora, aplicando el algoritmo de la división a $g(x)$ y $r(x)$, se obtiene

$$g(x) = r(x) \cdot q_1(x) + r_1(x),$$

donde $r_1(x)$ es cero, o de grado menor que el grado de $r(x)$. Si $r_1(x) = 0$, entonces $r(x)$ es un máximo común divisor de $f(x)$ y $g(x)$. Si $r_1(x) \neq 0$, entonces se tiene, tal y como se obtuvo anteriormente, que un m.c.d. de $g(x)$ y $r(x)$ es un m.c.d. de $r(x)$ y $r_1(x)$, reduciéndose el problema de encontrar un m.c.d. de $f(x)$ y $g(x)$ al problema de encontrar un m.c.d. de $r(x)$ y $r_1(x)$. Puede continuarse de esta manera, obteniéndose la sucesión de ecuaciones

$$\begin{aligned} f(x) &= g(x) \cdot q(x) + r(x), \\ g(x) &= r(x) \cdot q_1(x) + r_1(x), \\ r(x) &= r_1(x) \cdot q_2(x) + r_2(x), \\ r_1(x) &= r_2(x) \cdot q_3(x) + r_3(x), \\ &\ \ \vdots \end{aligned}$$

$$(4) \qquad r_j(x) = r_{j+1}(x) \cdot q_{j+2}(x) + r_{j+2}(x)$$
$$\vdots$$
$$r_{n-2}(x) = r_{n-1}(x) \cdot q_n(x) + r_n(x),$$
$$r_{n-1}(x) = r_n(x) \cdot q_{n+1}(x).$$

Este proceso muestra que, finalmente, debe obtenerse un residuo cero puesto que un residuo dado $r_j(x)$ es cero o de grado menor que el grado del residuo precedente $r_{j-1}(x)$. Obsérvese que un polinomio de grado cero, es decir, un elemento del campo, divide a todo polinomio sobre el campo. De aquí que, si el proceso no finaliza antes de obtener un polinomio de grado cero, el paso siguiente asegura la obtención de un residuo cero. El último residuo diferente de cero, $r_n(x)$, es un m.c.d. de $f(x)$ y $g(x)$ porque, denotando un m.c.d. de $f(x)$ y $g(x)$ por (f, g), se tiene $(f, g) = (g, r) = (r, r_1) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n$.

En el cálculo real de un m.c.d. de dos polinomios, puede simplificarse el trabajo multiplicando uno o más de los residuos, o los polinomios dados, por un elemento diferente de cero del campo. Puesto que todos los m.c.d. son asociados, esta multiplicación no cambia el m.c.d. El último residuo simplemente se multiplica por un elemento del campo. Además, debe observarse que el proceso de encontrar un m.c.d. solamente está relacionado con operaciones racionales realizadas con los coeficientes de los polinomios dados. Por lo tanto, los coeficientes de un m.c.d. siempre son elementos en el menor campo que contenga los coeficientes del polinomio dado.

Teorema 3. Sea d(x) *un m.c.d. de los dos polinomios* f(x) *y* g(x) *sobre el campo* F. *Entonces existen los polinomios* m(x) *y* n(x) *sobre* F, *tales que*

$$d(x) = m(x) \cdot g(x) + n(x) \cdot f(x).$$

Esta afirmación puede probarse expresando los residuos sucesivos de las ecuaciones (4) en términos de $f(x)$ y $g(x)$, así:

$$r(x) = f(x) - g(x) \cdot q(x),$$
$$r_1(x) = g(x) - r(x) \cdot q_1(x) = g(x) - q_1(x)[f(x) - g(x) \cdot q(x)]$$
$$= -q_1(x) \cdot f(x) + [1 + q(x) \cdot q_1(x)]g(x), \text{ etc.}$$

Puede darse una demostración general por inducción. Sea

$$r_j(x) = m_j(x) \cdot g(x) + n_j(x) \cdot f(x)$$

para todo $j > k$. Denotando $r(x)$ por $r_0(x)$, se ve que $r_j(x)$ se ha expresado en la forma deseada para $j = 0, 1$. A partir de las ecuaciones (4), se tiene

$$r_{k-2}(x) = r_{k-1}(x)\, q_k(x) \cdot + r_k(x).$$

Resolviendo esta ecuación para $r_k(x)$ y sustituyendo los valores para $r_{k-1}(x)$ y $r_{k-2}(x)$, dados por la hipótesis de inducción, se tiene

$$\begin{aligned} r_k(x) &= -q_k(x)[m_{k-1}(x) \cdot g(x) + n_{k-1}(x) \cdot f(x)] \\ &\qquad + [m_{k-2}(x) \cdot g(x) + n_{k-2}(x) \cdot f(x)] \\ &= [-q_k(x) \cdot m_{k-1}(x) + m_{k-2}(x)]g(x) + [-q_k(x) \cdot n_{k-1}(x) \\ &\qquad + n_{k-2}(x)]f(x), \end{aligned}$$

y se completa la inducción.

DEFINICIÓN. Se dice que dos polinomios $f(x)$ y $g(x)$ sobre un campo F son *relativamente primos* si su máximo común divisor es el elemento unidad de F.

EJEMPLO. Encontrar el m.c.d. de los dos polinomios $f(x) = x^5 + x^3 + x^2 + 2x + 3$ y $g(x) = x^4 + x^3 + 4x^2 + 3x + 3$ sobre el campo de clases de residuos módulo 5 y expresarlo en la forma $m(x) \cdot g(x) + n(x) \cdot f(x)$. Se encuentra que

$$f(x) = g(x)(x + 4) + 4x^3 + 2x^2 + 2x + 1,$$
$$g(x) = (4x^3 + 2x^2 + 2x + 1)(4x + 2) + 2x^2 + 1,$$
$$4x^3 + 2x^2 + 2x + 1 = (2x^2 + 1)(2x + 1).$$

Por lo tanto, $2x^2 + 1$ es un m.c.d. y su asociado mónico, $x^2 + 3$, es el m.c.d. Para expresar el m.c.d., en la forma deseada, se aplican las ecuaciones anteriores, obteniendo

$$\begin{aligned} 2x^2 + 1 &= g(x) - (4x^3 + 2x^2 + 2x + 1)(4x + 2) \\ &= g(x) - [f(x) - g(x)(x + 4)](4x + 2) \\ &= (4x^2 + 3x + 4)g(x) - (4x + 2)f(x), \end{aligned}$$

y

$$x^2 + 3 = (2x^2 + 4x + 2)g(x) + (3x + 4)f(x).$$

Ejercicios

1. Encontrar el máximo común divisor de los dos polinomios $f(x)$ y $g(x)$ sobre el campo de coeficientes indicado y expresarlo en la forma $m(x) \cdot g(x) + n(x) \cdot f(x)$.

   a. $f(x) = x^5 - x^4 - 6x^3 - 2x^2 + 5x + 3$, $\quad g(x) = x^3 - 3x - 2$ sobre el campo de los números racionales.

b. $f(x) = x^4 - 5x^3 + 6x^2 + 4x - 8$, $g(x) = x^3 - x^2 - 4x + 4$ sobre el campo de los números racionales.
c. $f(x) = x^3 - 4ix + 3$, $g(x) = x^2 - i$ sobre el campo de los números complejos.

2. Encontrar el m.c.d. de los siguientes pares de polinomios sobre el campo de los números racionales:

a. $f(x) = 4x^4 - 4x^3 + 5x^2 - 4x + 1$, $g(x) = 8x^3 - 6x^2 + 5x - 2$.
b. $f(x) = x^4 + x^3 + 2x^2 + x + 1$, $g(x) = x^3 - 1$.

3. Encontrar el m.c.d. de los siguientes pares de polinomios sobre el campo de las clases de residuos módulo 3:

a. $f(x) = x^5 + 2x^3 + x^2 + 2x$, $g(x) = x^4 + x^3 + x^2$.
b. $f(x) = x^3 + 2x^2 + 2x + 1$, $g(x) = x^2 + 2$.

4. Determinar la constante c si el máximo común divisor de $f(x)$ y $g(x)$ sobre el campo de los números racionales es lineal. Para cada valor de c obtenido, ¿cuál es el máximo común divisor?

a. $f(x) = x^3 + cx^2 - x + 2c$, $g(x) = x^2 + cx - 2$.
b. $f(x) = x^2 + (c - 6)x + 2c - 1$, $g(x) = x^2 + (c + 2)x + 2c$.

4 · TEOREMAS DE FACTORIZACION

Continuaremos con la lista de todos aquellos teoremas para los polinomios sobre un campo, que son análogos a los teoremas probados para los enteros.

Teorema 4. Si p(x) *es un polinomio irreducible sobre un campo* F *y si* p(x) *divide al producto* f(x) · g(x) *de dos polinomios sobre* F, *entonces* p(x) *divide a* f(x) *o* p(x) *divide a* g(x).

Supóngase que $p(x)$ no divide a $f(x)$. Suponiendo que $p(x)$ es irreducible sobre F, sus únicos divisores son sus asociados y los unitarios del campo. De aquí que $p(x)$ y $f(x)$ son primos relativamente y su m.c.d. es el elemento unidad u del campo. Por lo tanto, existen los polinomios $m(x)$ y $n(x)$ sobre F tales que

$$u = m(x) \cdot p(x) + n(x) \cdot f(x).$$

Multiplíquese esta ecuación por $g(x)$ para obtener

$$g(x) = m(x) \cdot p(x) \cdot g(x) + n(x) \cdot f(x) \cdot g(x).$$

Aplicando la hipótesis de que $p(x)$ divide a $f(x) \cdot g(x)$, se ve que $p(x)$ es un factor del segundo miembro de la ecuación anterior. De aquí

que también es un factor del primer miembro de la ecuación, y se establece el teorema.

Se dejan al estudiante las demostraciones de los dos teoremas siguientes.

Teorema 5. Si un polinomio irreducible p(x) *sobre un campo* F *divide el producto de* n *polinomios* $q_1(x) \cdot q_2(x) \cdots q_n(x)$ *sobre* F, *divide a algún factor* $q_i(x)$.

Teorema 6. Si f(x) *y* g(x) *son polinomios primos relativamente sobre un campo* F, *y si* f(x) *divide al producto* g(x) · h(x), *entonces* f(x) *divide a* h(x).

Teorema 7. Teorema de la factorización única. Un polinomio f(x) *de grado positivo sobre un campo* F, *puede expresarse como un elemento de* F *multiplicado por un producto de polinomios mónicos irreducibles sobre* F. *Esta descomposición es única excepto en el orden en que se presentan los factores.*

Primero, se probará que esa descomposición es posible. Si $f(x)$ es irreducible, la descomposición está realizada. (Obsérvese que si $f(x)$ es de grado 1, es irreducible). Ahora, supóngase que $f(x)$ es reducible de modo que $f(x) = g(x) \cdot h(x)$, donde $g(x)$ y $h(x)$ son polinomios de grado menor que el grado de $f(x)$. Hacemos la hipótesis de inducción de que la descomposición es posible para todos los polinomios de grado menor que el grado de $f(x)$. Por lo tanto

$$g(x) = cp_1(x) \cdot p_2(x) \cdots p_r(x)$$

y

$$h(x) = c'p_1'(x) \cdot p_2'(x) \cdots p_s'(x),$$

donde c y c' son elementos del campo y donde los $p_i(x)$ y $p_i'(x)$ son polinomios mónicos irreducibles sobre F. Entonces, se tiene

$$f(x) = g(x) \cdot h(x) = cc'p_1(x) \cdots p_r(x) \cdot p_1'(x) \cdots p_s'(x).$$

Por lo tanto, la inducción se completa y la descomposición se realiza.

Falta por probar que la descomposición es única. Supóngase la existencia de dos descomposiciones

$$\begin{aligned} f(x) &= cp_1(x) \cdot p_2(x) \cdots p_n(x) \\ &= dq_1(x) \cdot q_2(x) \cdots q_m(x). \end{aligned}$$

Puesto que estos polinomios irreducibles son mónicos $c = d$. Puesto que $p_1(x)$ es irreducible, divide a algunos $q_i(x)$. Como $p_1(x)$ y $q_i(x)$ son mónicos e irreducibles, su cociente es el elemento unidad del campo y de aquí que $p_1(x) = q_i(x)$. Dividiendo entre este factor común y c, se obtiene

$$f_1(x) = p_2(x) \cdots p_n(x) = q_1(x) \cdots q_{i-1}(x) \cdot q_{i+1}(x) \cdots q_m(x).$$

Ahora, $f_1(x)$ es un polinomio de grado menor que el grado de $f(x)$. En consecuencia, puede hacerse una hipótesis de inducción para el efecto de que la descomposición es única para todos los polinomios de grado menor de $f(x)$. Por lo tanto, la descomposición de $f_1(x)$ es única, $n = m$, y los dos conjuntos de polinomios son idénticos. De aquí que se tiene la descomposición única de $f(x)$.

Ejercicios

1. Probar los teoremas 5 y 6.
2. Hacer una lista de los polinomios mónicos de segundo grado sobre el campo de las clases de residuos módulo 3. ¿Cuáles son irreducibles? Encontrar la descomposición de los polinomios reducibles.
3. Encontrar la descomposición de los siguientes polinomios sobre el campo de los números racionales y sobre el campo de los números complejos: (a) $x^3 - 1$, (b) $x^4 - 1$, (c) $x^6 - 1$. (*Sugerencia:* Recuérdese que los ceros de estos polinomios son raíces de la unidad).
4. Encontrar la descomposición de los siguientes polinomios sobre el campo de las clases de residuos módulo 3: (a) $x^3 + x + 2$; (b) $2x^3 + x^2 + 1$.
5. Demostrar que $x^2 + x + 1$ es un polinomio irreducible sobre el campo de las clases de residuos módulo 5.
6. Si $h(x)$ es relativamente primo tanto a $f(x)$ como a $g(x)$, sobre un campo F, probar que $h(x)$ es relativamente primo al producto $f(x) \cdot g(x)$.

5 · CEROS DE UN POLINOMIO

Teorema 8. Un polinomio $f(x)$ *de grado positivo* n *sobre un campo* F *tiene cuando más* n *ceros en* F.

Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n$, con $a_n \neq 0$. Si $f(x)$ tiene un cero r_1, el teorema del factor nos da $f(x) = (x - r_1)q(x)$. Mediante una sustitución se ve que un cero de $q(x)$ es un cero de $f(x)$. Por lo tanto, $f(x)$ tiene como ceros a r_1 y a los ceros de $q(x)$. Por otra parte, $f(x)$ no tiene otros ceros que no sean r_1 y los ceros de $q(x)$, porque si a fuera un cero de $f(x)$, que no sea r_1 ni un cero de $q(x)$, podría tenerse $f(a) = 0 = (a - r_1)q(a)$. Puesto que ni $q(a)$ ni $a - r_1$ son cero y puesto que no existen divisores propios de cero en un campo, esta igualdad es imposible. Ahora, puede hacerse la prueba por inducción. El polinomio $q(x)$ es de grado $n - 1$ y de aquí que se hace la hipótesis de inducción de que $q(x)$ tiene cuando más $n - 1$ ceros. Así, $f(x)$ tiene cuando más n ceros y se completa la prueba observando que un polinomio de grado 1, $a_0 + a_1x (a_1 \neq 0)$ tiene sólo un cero, $-a_0/a_1$.

Teorema 9. Si el polinomio $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *sobre un campo* F, *tiene los* n *ceros* $r_1, r_2, \cdots, r_n$ *en* F, *entonces* $f(x)$ *puede escribirse unívocamente como* $a_n(x - r_1)(x - r_2) \cdots (x - r_n)$.

Puesto que r_1 es un cero, $f(x) = (x - r_1)q(x)$. De acuerdo con el teorema 8, los ceros de $f(x)$ son r_1 y los ceros de $q(x)$. Si $f(x)$ es de grado 1, $q(x)$ es un elemento de F y, evidentemente, el teorema se cumple. Por tanto, supondremos que $f(x)$ es de grado mayor que 1 y que los ceros de $q(x)$ son $r_2, r_3, \cdots, r_n$. Ahora, hacemos la hipótesis de inducción de que si un polinomio de grado $m < n$ tiene m ceros puede escribirse en forma factorizada. Obsérvese que $q(x)$ es de grado $n - 1$ y que el coeficiente de su mayor potencia de x es a_n. Por lo tanto, $q(x) = a_n(x - r_2)(x - r_3) \cdots (x - r_n)$ y $f(x) = (x - r_1)q(x)$ tiene la forma factorizada requerida. El teorema de la factorización única nos dice que esta descomposición es única porque los $x - r_i$ son polinomios mónicos irreducibles sobre F.

Daremos sin demostración * el llamado teorema fundamental del álgebra.

Teorema 10. Un polinomio de grado positivo sobre el campo de los números complejos tiene un cero que es un número complejo.

Teorema 11. Un polinomio $f(x) = a_0 + a_1x + \cdots + a_nx^n$, *con* $a_n \neq 0$, *sobre el campo de los números complejos, tiene exactamente* n *ceros que son números complejos.*

Si $n = 1$, $f(x) = a_0 + a_1x$, y el teorema evidentemente se cumple. Si $n > 1$, se observa que, de acuerdo con el teorema fundamental del álgebra, $f(x)$ tiene un cero r_1 que es un número complejo. De aquí que $f(x) = (x - r_1)q(x)$. Además, $q(x)$ es de grado $n - 1$ y, si $n - 1 > 0$, $q(x)$ tiene una raíz r_2 que es un número complejo. Hacemos la

* Todas las demostraciones están relacionadas con conceptos no algebraicos (por ejemplo, la continuidad). Ver, por ejemplo, G. D. Birkhoff y S. MacLane, *A Survey of Modern Algebra* (edición revisada), Nueva York, The Macmillan Co., 1953, págs. 107-109.

hipótesis de inducción de que un polinomio de grado $m < n$ sobre el campo de los números complejos tiene exactamente m ceros. De aquí que $q(x)$ tiene exactamente $n - 1$ ceros y $f(x)$ tiene exactamente n ceros, lo que debía demostrarse.

De aquí que, de acuerdo con el teorema 9, $f(x)$ puede escribirse unívocamente en la forma $f(x) = a_n(x - r_1)(x - r_2) \cdots (x - r_n)$. Por lo tanto, los únicos polinomios mónicos irreducibles sobre el campo de los números complejos son lineales.

Ahora, particularicemos el campo de coeficientes al campo de los números reales y se ve que la descomposición está dada por el teorema de la factorización única.

Teorema 12. Si un polinomio $f(x)$ *sobre el campo de los números reales tiene el cero* $a + bi$, *donde* $b \neq 0$, *tiene el cero conjugado* $a - bi$.

Fórmese el producto $[x - (a + bi)][x - (a - bi)] = (x - a)^2 + b^2$ del cual se observa que es un polinomio con coeficientes reales. De aquí que, cuando se divide $f(x)$ entre este polinomio, se obtiene un cociente y un residuo sobre el campo de los números reales. Por lo tanto, $f(x) = [(x - a)^2 + b^2]q(x) + r(x)$, donde $r(x)$ es cero o cuando más de grado 1. Por supuesto que se desea probar que $r(x) = 0$. Sea $r(x) = mx + n$. Ahora, $f(a + bi) = 0 = m(a + bi) + n$. Por lo tanto, $ma + n = 0$ y $mb = 0$. Puesto que $b \neq 0$, $m = 0$ y de aquí que $n = 0$. Así, $r(x) = 0$ y $f(x)$ tiene el factor $x - (a - bi)$ si tiene el factor $x - (a + bi)$. (Otra demostración de este teorema se dará en el Cap. 9).

Recuérdese que un polinomio cuadrático $ax^2 + bx + c$ sobre el campo de los números reales no tiene ceros reales si su discriminante $b^2 - 4ac < 0$. Así, los polinomios cuadráticos reales con discriminantes negativos son irreducibles sobre el campo de los números reales. Ahora, considérese un polinomio con coeficientes reales como un polinomio sobre el campo de los números complejos. Entonces, tiene una factorización en factores lineales. El teorema 12 nos dice que todo factor lineal correspondiente a un cero de la forma $a + bi (b \neq 0)$ puede parearse con un factor lineal correspondiente al cero conjugado $a - bi$ y que el producto de dos factores lineales de este tipo es un polinomio cuadrático real. De aquí que se tenga el teorema siguiente.

Teorema 13. Un polinomio sobre el campo de los números reales puede escribirse unívocamente como el producto de un número real por un producto de factores cuadráticos mónicos irreducibles y reales y factores lineales mónicos reales.

Para un polinomio sobre el campo de los números racionales, el teorema siguiente nos proporciona un medio para determinar sus ceros racionales. Este teorema y su corolario en ocasiones ayudan a determinar si un polinomio sobre el campo de los números racionales es reducible. Primero, obsérvese que al multiplicar por el entero apropiado se sustituye un polinomio con coeficientes racionales por un asociado que tiene coeficientes enteros. Por lo tanto, el problema se reduce al de encontrar los ceros racionales de un polinomio con coeficientes enteros.

Teorema 14. Sea c/d, *donde* $(c, d) = 1$, *un cero racional del polinomio* $a_0 + a_1x + \cdots + a_nx^n$ *con coeficientes enteros. Entonces* c *divide a* a_0 *y* d *divide a* a_n.

Ahora, $a_0 + a_1(c/d) + \cdots + a_{n-1}(c/d)^{n-1} + a_n(c/d)^n = 0$ y de aquí que el entero

$$(5) \qquad a_0d^n + a_1cd^{n-1} + \cdots + a_{n-1}c^{n-1}d + a_nc^n = 0.$$

Por tanto, $d(a_0d^{n-1} + a_1cd^{n-2} + \cdots + a_{n-1}c^{n-1}) + a_nc^n = 0$ y d divide a a_nc^n. Sin embargo, $(c^n, d) = 1$ (ver ejercicio 7, pág. 30) y de aquí que d divide a a_n. En forma semejante, el entero (5) puede escribirse $a_0d^n + c(a_1d^{n-1} + \cdots + a_nc^{n-1}) = 0$ y c divide a a_0d^n, pero, asimismo, $(c, d^n) = 1$ y de aquí que c divide a a_0.

Corolario. Todos los ceros racionales del polinomio $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ *con coeficientes enteros son enteros y divisores de* a_0.

El corolario se sigue del teorema cuando se observa que d divide a $a_n = 1$.

Se observa que el corolario anterior nos proporciona una forma sencilla de probar que ciertos números reales tales como $\sqrt{3}$ y $\sqrt[3]{5}$ son irracionales porque son ceros, respectivamente, de los polinomios $x^2 - 3$ y $x^3 - 5$. Fácilmente se comprueba que estos polinomios no tienen ceros racionales.

EJEMPLO. Encontrar los ceros racionales y la descomposición del polinomio $f(x) = 6x^4 - 7x^3 + 6x^2 - 1$ sobre el campo de los números racionales. De acuerdo con el teorema anterior, los ceros racionales posibles son ± 1, $\pm 1/2$, $\pm 1/3$, $\pm 1/6$. Aplicando la división sintética se encuentra que ± 1 no son ceros pero que $1/2$ es un cero:

$$\begin{array}{rrrrr|l} 6 & -7 & 6 & 0 & -1 & \tfrac{1}{2} \\ & 3 & -2 & 2 & 1 & \\ \hline 6 & -4 & 4 & 2 & 0. & \end{array}$$

Como ahora se sabe que $f(x) = (x - 1/2)(6x^3 + 4x^2 + 4x + 2)$, se aplica el cociente dividido entre 2, a saber $3x^3 - 2x^2 + 2x + 1$, para descubrir los ceros racionales restantes de $f(x)$. Ahora, solamente es necesario intentar $\pm 1/3$. Se encuentra que $-1/3$ es un cero y que $3x^2 - 3x + 3$ es el segundo cociente. Puesto que $x^2 - x + 1$ no tiene ceros racionales, $6(x - 1/2)(x + 1/3)(x^2 - x + 1)$ es la descomposición de $f(x)$ sobre el campo de los números racionales.

Ejercicios

1. Encontrar la descomposición del polinomio $x^4 + 9x^3 + 28x^2 + 36x + 16$ sobre el campo de los números racionales.
2. Encontrar la descomposición del polinomio $4x^4 + 8x^3 + 7x^2 + 8x + 3$ sobre el campo de los números racionales y sobre el campo de los números complejos.
3. Encontrar la descomposición del polinomio $x^3 - 25x - 48$ sobre el campo de los números racionales y sobre el campo de los números reales.
4. Encontrar la descomposición de $x^8 - 1$ sobre el campo de los números complejos y sobre el campo de los números reales.
5. Encontrar las descomposiciones de $x^8 - 1$ y $x^{12} - 1$ sobre el campo de los números complejos, sobre el campo de los números reales y sobre el campo de los números racionales.
6. Encontrar la descomposición sobre el campo de las clases de residuos módulo 5 del polinomio $2x^3 + 3x^2 + 3x + 1$.
7. Encontrar el máximo común divisor de $2x^4 + 9x^2 + 17x - 21$ y $x^3 + 2x^2 + 4x + 21$. De aquí, encontrar la descomposición del primer polinomio sobre el campo de los números reales y sobre el campo de los números complejos.
8. Encontrar los ceros de los polinomios siguientes sobre el campo de los números y expresar cada cero en la forma $a + bi$, siendo a y b números reales.
   a. $x^2 + ix + 1$.
   b. $x^2 - x + i$.
   c. $x^2 - ix + i$.
   d. $x^2 + \sqrt{2}x + 2i$.

6 · RELACION ENTRE LOS CEROS Y LOS COEFICIENTES DE UN POLINOMIO

En todo campo F en el cual el polinomio

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

sobre F tiene la descomposición

$$f(x) = a_n(x - r_1)(x - r_2)\cdots(x - r_n),$$

existen ciertas relaciones entre los coeficientes del polinomio y sus ceros que se describirán a continuación. Las combinaciones siguientes de los ceros $r_1, r_2, \cdots, r_n$ reciben el nombre de *funciones simétricas elementales* de $r_1, r_2, \cdots, r_n$:

$$S_1 = r_1 + r_2 + \cdots + r_n = \sum r_1,$$
$$S_2 = r_1r_2 + r_1r_3 + \cdots + r_{n-1}r_n = \sum r_1r_2,$$
$$\cdots\cdots\cdots$$
$$S_n = r_1r_2r_3\cdots r_n.$$

Por lo tanto, la j-ésima función simétrica elemental es la suma de los productos, consistente cada uno de j factores distintos, que pueden formarse a partir de los ceros $r_1, r_2, \cdots, r_n$. De aquí que existen $C(n, j) = n!/[(n - j)!j!]$ términos en la j-ésima función simétrica elemental. Estas funciones reciben el nombre de funciones simétricas porque no cambian o son invariantes cuando se operan por los elementos del grupo simétrico en n símbolos.

Para obtener las relaciones deseadas, a continuación se probará el siguiente lema.

Lema

(6) $$(x - r_1)(x - r_2)\cdots(x - r_n) = x^n - S_1x^{n-1} + S_2x^{n-2} + \cdots + (-1)^jS_jx^{n-j} + \cdots + (-1)^nS_n.$$

Obsérvese que, cuando $n = 1$, $x - r_1 = x - S_1$ y cuando $n = 2$,

$$(x - r_1)(x - r_2) = x^2 - (r_1 + r_2)x + r_1r_2 = x^2 - S_1x + S_2,$$

donde los símbolos S_1 y S_2 denotan las funciones simétricas elementales de una y dos variables, respectivamente. Por lo tanto, el lema es verdadero para $n = 1$ y $n = 2$ y se completa la prueba por inducción.

Supóngase que el lema es verdadero para $n = k$:

(7) $$(x - r_1)(x - r_2)\cdots(x - r_k) = x^k - S_1x^{k-1} + S_2x^{k-2} + \cdots + (-1)^jS_jx^{k-j} + \cdots + (-1)^kS_k.$$

Aquí S_j es la j-ésima función simétrica elemental de $r_1, r_2, \cdots, r_k$. Multiplíquense ambos miembros de la ecuación (7) por $x - r_{k+1}$, obteniendo

(8) $$(x - r_1)(x - r_2)\cdots(x - r_k)(x - r_{k+1}) = x^{k+1} - (S_1 + r_{k+1})x^k + (S_2 + r_{k+1}S_1)x^{k-1} + \cdots + (-1)^j(S_j + r_{k+1}S_{j-1})x^{k-j+1} + \cdots + (-1)^{k+1}r_{k+1}S_k.$$

Sean $S_1', S_2', \cdots, S'_{k+1}$ las funciones simétricas elementales de $r_1, r_2, \cdots, r_k, r_{k+1}$. Entonces $S_1' = S_1 + r_{k+1}$, $S_2' = S_2 + r_{k+1}S_1, \cdots, S_j' = S_j + r_{k+1}S_{j-1}$.

Puesto que se observa que la suma de los productos, cada uno de j factores distintos, de $r_1, r_2, \cdots, r_k, r_{k+1}$ es la suma de los productos, cada uno de j factores distintos, de $r_1, r_2, \cdots, r_k$ más r_{k+1} multiplicado por la suma de los productos, cada uno de $j-1$ factores, de estos ceros. Por lo tanto, (8) es de la forma (6) con $n = k+1$, y se completa la inducción.

Ahora,

$$f(x) = a_0 + a_1x + \cdots + a_nx^n = a_n(x-r_1)(x-r_2)\cdots(x-r_n)$$
$$= a_n[x^n - S_1x^{n-1} + \cdots + (-1)^nS_n],$$

e igualando la primera y la última formas del polinomio, se tiene el teorema siguiente:

Teorema 15. Si $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *sobre un campo* F *tiene los* n *ceros* $r_1, r_2, \cdots, r_n$ *en* F, *entonces* $S_j = (-1)^j a_{n-j}/a_n$, $j = 1, 2, \cdots, n$.

Ejercicios

1. Aplicando la relación entre los ceros y los coeficientes de un polinomio, encontrar un polinomio sobre el campo de los números racionales cuyos ceros sean: (a) $-1, 2, 3$; (b) $2, 2, 2$; (c) $0, 0, 1, 2$; (d) $-1, -1, 3, 4$.
2. Denotar los ceros de los polinomios siguientes por r_1, r_2, r_3, r_4. Encontrar los valores de las funciones simétricas elementales para cada uno de los polinomios:
   a. $x^4 + 4x^3 - 2x + 3$.
   b. $4x^4 + 4x^3 + x^2 - x + 2$.
   c. $3x^4 - 4x^2 + 2$.
3. Si r_1, r_2, r_3 son los ceros de $x^3 - 3x^2 + 2x + 1$, encontrar un polinomio cuyos ceros sean $2r_1, 2r_2, 2r_3$.
4. Sean r_1, r_2, r_3 los ceros del polinomio $2x^3 - 3x^2 + kx - 1$. Determinar la constante k si la suma de dos de ellos es 2. Encontrar los ceros del polinomio resultante.
5. Sean r_1, r_2, r_3 los ceros del polinomio $\sqrt{2}x^3 + kx^2 - 2\sqrt{2}x + 2$. Determinar la constante k si el producto de dos de los ceros es 1. Encontrar los ceros del polinomio resultante.
6. Determinar k de modo que un cero del polinomio $3x^3 - kx^2 - 7x + 3$ sea el recíproco de otro. De aquí, determinar los ceros del polinomio.

7 · DERIVADA DE UN POLINOMIO

Formalmente se define la derivada de $f(x) = a_0 + a_1x + \cdots + a_nx^n$ como $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$. (Por supuesto que aquí $2a_2$ significa $a_2 + a_2$, $3a_3$ significa $a_3 + a_3 + a_3$, etc.) Esta definición puede

aplicarse para probar las fórmulas usuales para las derivadas de sumas, productos y potencias de polinomios, y se aplicarán estas fórmulas. Obsérvese, por ejemplo, que, si el polinomio es un polinomio sobre el campo de los números complejos, los únicos polinomios cuyas derivadas son cero son las constantes. Sin embargo, si, por ejemplo, $f(x) = x^p$ se considera como un polinomio sobre el campo de las clases de residuos módulo p, donde p es primo, $f(x)$ tiene la derivada px^{p-1}, la cual es cero. Los resultados debidos a la aplicación de las derivadas dependen de si la derivada de un polinomio únicamente es cero cuando el polinomio es un elemento en un campo o si también puede ser cero cuando el polinomio es de grado positivo. Para evitar esta complicación, *restringiremos nuestro campo de coeficientes al campo de los números complejos o a uno de sus subcampos.* El estudiante que se interese en este tema puede leer en textos más avanzados lo que puede probarse cuando no se hace esta restricción.

Ejercicios

1. Encontrar la derivada de los polinomios siguientes:
   a. $3x^3 + 2x^2 + x + 5$.
   b. $2x^4 - 3x^2 + x - 2$.
   c. $5x^3 - 3x^2 + 2$.
   d. $7x^5 - 2x^3 - x^2 + 5$.
2. Probar que, si $f(x)$ y $g(x)$ son polinomios y $h(x) = f(x) + g(x)$, entonces $h'(x) = f'(x) + g'(x)$.
3. Porbar que, si $f(x)$ y $g(x)$ son polinomios y $h(x) = f(x)g(x)$, entonces $h'(x) = f(x)g'(x) + g(x)f'(x)$.
4. Probar que, si $f(x)$ es un polinomio, n es un entero positivo y $g(x) = [f(x)]^n$, entonces $g'(x) = n[f(x)]^{n-1}f'(x)$.

8 · FACTORES MULTIPLES

DEFINICIONES. Si el polinomio $[p(x)]^m$ divide al polinomio $f(x)$ y si ninguna potencia superior de $p(x)$ divide a $f(x)$, se dice que $p(x)$ es un *factor de multiplicidad m* de $f(x)$. *Si* $(x-a)^m$ divide al polinomio $f(x)$ y si ninguna potencia superior de $x - a$ divide a $f(x)$, a recibe el nombre de *cero de multiplicidad m.*

En los teoremas siguientes se restringirá el campo de coeficientes del polinomio $f(x)$ al campo de los números complejos o a uno de sus subcampos.

Teorema 16. Sea p(x) *un factor irreducible de* f(x) *de multiplicidad* m > 1. *Entonces* $[p(x)]^{m-1}$ *es la mayor potencia de* p(x) *que se*

presenta como factor del máximo común divisor de f(x) *y su derivada* f′(x). *Recíprocamente, si el máximo común divisor de* f(x) *y* f′(x) *tiene el factor irreducible* p(x) *como un factor de multiplicidad* m − 1, p(x) *es un factor irreducible de* f(x) *de multiplicidad* m.

Primero, sea $p(x)$ un factor irreducible de multiplicidad m de $f(x)$. Entonces, puede escribirse $f(x) = [p(x)]^m q(x)$, donde $p(x)$ y $q(x)$ son primos relativamente, puesto que $f(x)$ tiene una factorización única en polinomios irreducibles. Aplicando las reglas comunes para la derivación se tiene

$$f'(x) = [p(x)]^{m-1}[mp'(x) \cdot q(x) + p(x) \cdot q'(x)].$$

Es obvio que $[p(x)]^{m-1}$ es un factor común de $f(x)$ y $f'(x)$ y de aquí que divide a su m.c.d. Se demuestra que ninguna potencia superior de $p(x)$ se presenta como un factor del m.c.d., probando que $m - 1$ es la mayor potencia de $p(x)$ que divide a $f'(x)$. Ahora, $p(x)$ es primo relativamente a su derivada $p'(x)$ porque $p'(x)$ es de grado menor que el grado de $p(x)$ y de aquí que no puede tener factor común con el polinomio irreducible $p(x)$. Así, $p(x)$ no divide al segundo factor de $f'(x)$ puesto que es primo relativamente a $p'(x) \cdot q'(x)$ y divide a $p(x) \cdot q'(x)$. De aquí que $m - 1$ es la mayor potencia de $p(x)$ que divide al m.c.d. de $f(x)$ y $f'(x)$.

Falta por probar el inverso. Ahora, considérese que el m.c.d. de $f(x)$ y $f'(x)$ tiene el factor irreducible $p(x)$ de multiplicidad $m - 1$. Sea k la mayor potencia de $p(x)$ que divide a $f(x)$. Aplicando el teorema de la factorización única, una vez más, se tiene $f(x) = [p(x)]^k q(x)$, donde $p(x)$ y $q(x)$ son polinomios relativamente primos. De acuerdo con la demostración anterior, el m.c.d. de $f(x)$ y $f'(x)$ tiene a $p(x)$ como un factor irreducible de multiplicidad $k - 1$. De aquí que $k - 1 = m - 1$ y $k = m$, lo que debía demostrarse.

Corolario 1. Un polinomio f(x) *no tiene factores repetidos de multiplicidad mayor que* 1 *si y solamente si él y su derivada son primos relativamente.*

Se ve fácilmente que este corolario es cierto cuando se considera que todo factor de $f(x)$ puede descomponerse en sus factores irreducibles.

Corolario 2. Si r *es un cero de multiplicidad* m *del m.c.d. de* f(x) *y su derivada, entonces* r *es un cero de multiplicidad* m + 1 *de* f(x).

Este corolario es inmediato a partir del teorema porque un cero de un polinomio corresponde a un factor lineal irreducible del polinomio.

Para demostrar que este teorema no puede aplicarse a un polinomio sobre cualquier campo de coeficientes, considérese el polinomio $f(x) = x^3 - 1$ sobre el campo de clases de residuos módulo 3. Se ve que $x^3 - 1 = (x - 1)^3$ y de aquí que $x^3 - 1$ tiene un factor irreducible de multiplicidad 3. Sin embargo, $f'(x) = 3x^2 = 0$.

EJEMPLO. Determinar si el polinomio $f(x) = x^4 + 2x^3 - 2x - 1$ tiene algún factor irreducible de multiplicidad mayor que 1. Si los tiene, encontrarlos y de ahí encontrar la descomposición del polinomio sobre el campo de los números racionales.

Ahora, $f'(x) = 4x^3 + 6x^2 - 2$ y $4f(x) = f'(x) \cdot (x + 1/2) - 3(x^2 + 2x + 1)$. El m.c.d. de $f(x)$ y $f'(x)$ divide a $(x + 1)^2$, el residuo mónico cuando $4f(x)$ se divide entre $f'(x)$. De aquí que, si existe un factor irreducible de multiplicidad mayor que 1 de $f(x)$, debe ser $x + 1$. Efectuando una división sintética se encuentra que $f(x) = 2(x + 1)^2(2x - 1)$. Por lo tanto, $f(x)$ tiene el factor $x + 1$ como un factor de multiplicidad 3 y mediante la división sintética se encuentra que $f(x) = (x + 1)^3(x - 1)$. (En cualquier paso del proceso de cálculo del máximo común divisor, el estudiante debe simplificar su trabajo observando los factores posibles del residuo).

Ejercicios

1. Determinar si los polinomios siguientes tienen ceros de multiplicidad mayor que 1. Si existen ceros de multiplicidad mayor que 1, encontrar todos los ceros del polinomio.

   a. $x^4 - 4x^3 + 5x^2 - 4x + 4$.
   b. $x^4 + 2x^3 - x^2 - 4x - 2$.
   c. $x^3 - 7x^2 + 15x - 9$.
   d. $8x^4 - 4x^3 - 6x^2 + 5x - 1$.

2. Encontrar la descomposición de los siguientes polinomios sobre el campo de los números racionales, el campo de los números reales y el campo de los números complejos:

   a. $x^5 - x^4 + 2x^3 - 2x^2 + x - 1$.
   b. $x^6 - 2x^4 - 4x^2 + 8$.

3. Demostrar que los siguientes polinomios no tienen factores repetidos:

   a. $x^n - a, \quad a \neq 0$. b. $x^3 - 6x + 1$.
   c. $x^5 + x^4 - 4x^2 + 4$. d. $x^6 - 6x^3 + 1$.

4. Encontrar la condición que deben satisfacer los coeficientes si los polinomios siguientes no tienen factores repetidos:

   a. $ax^2 + bx + c, \quad a \neq 0$.
   b. $x^3 + 3ax + b$.

5. ¿Para qué valores reales de a el polinomio $x^n + nax + n - 1$, donde $n > 1$, tiene un factor repetido?

9 · TEOREMA DE TAYLOR PARA LOS POLINOMIOS

Teorema 17. Sea f(x) *un polinomio de grado* n. *Entonces* $f(x+h) = f(h) + xf'(h) + x^2f''(h)/2! + \cdots + x^kf^{(k)}(h)/k! + \cdots + x^nf^{(n)}(h)/n!$

El polinomio $f(x+h)$ puede expresarse como un polinomio en x cuyos coeficientes son funciones de h y de los coeficientes de $f(x)$. Por lo tanto, sea

$$f(x+h) = b_0 + b_1x + b_2x^2 + \cdots + b_kx^k + \cdots + b_nx^n.$$

Sus derivadas sucesivas son:

$$f'(x+h) = b_1 + 2b_2x + 3b_3x^2 + \cdots + kb_kx^{k-1} + \cdots + nb_nx^{n-1},$$

$$f''(x+h) = 2b_2 + 3 \cdot 2b_3x + \cdots + k(k-1)b_kx^{k-2} + \cdots + n(n-1)b_nx^{n-2},$$

. . . .

$$f^{(k)}(x+h) = k!\,b_k + \cdots + n(n-1)\cdots(n-k+1)b_nx^{n-k},$$

. . . .

$$f^{(n)}(x+h) = n!\,b_n.$$

Para $x = 0$ se tiene $f(h) = b_0$, $f'(h) = b_1$, $f''(h) = 2b_2, \cdots, f^{(k)}(h) = k!b_k, \cdots, f^{(n)}(h) = n!b_n$. Sustituyendo estos valores de b_i en $f(x+h)$, se tiene el resultado deseado

$$f(x+h) = f(h) + xf'(h) + x^2\frac{f''(h)}{2!} + \cdots + x^n\frac{f^{(n)}(h)}{n!}.$$

Esta es una forma del teorema de Taylor para los polinomios. Si en ella se sustituye x por $x - h$, se tiene

$$f(x) = f(h) + (x-h)f'(h) + (x-h)^2\frac{f''(h)}{2!} + \cdots$$

$$+ (x-h)^k\frac{f^{(k)}(h)}{k!} + \cdots + (x-h)^n\frac{f^{(n)}(h)}{n!}$$

Esta segunda forma indica cómo pueden calcularse fácilmente los valores de $f(h), f'(h), f''(h)/2!, \cdots, f^{(n)}(h)/n!$ Aplicando esta segunda forma del teorema de Taylor se ve que cuando $f(x)$ se divide entre $x - h$, el residuo es $f(h)$ y el cociente es

$$f'(h) + (x-h)\frac{f''(h)}{2!} + \cdots + (x-h)^{n-1}\frac{f^{(n)}(h)}{n!}.$$

Si este cociente se divide entre $x - h$, el residuo es $f'(h)$. Puede continuarse en esta forma, dividiendo los cocientes sucesivos entre $x - h$ y obtener los coeficientes deseados $f''(h)/2!, \cdots, f^{(n)}(h)/n!$ El estudiante debe recordar que la forma más sencilla de dividir un polinomio entre $x - h$ es por división sintética.

Considérese la relación entre los ceros de $f(x)$ y los de $f(x+h)$. Sea x_1 un cero de $f(x)$. Por lo tanto, $x_1 - h$ es un cero de $f(x+h)$ puesto que $f(x_1 - h + h) = f(x_1) = 0$. Así cada cero de $f(x+h)$ es menor en h que el cero correspondiente de $f(x)$.

EJEMPLO. Se desea encontrar un polinomio en el que cada uno de sus ceros sean menores en 2 que los ceros de $f(x) = 3x^3 - 2x^2 - 5x - 1$. De acuerdo con la observación anterior se sabe que este problema es equivalente a encontrar $f(x+2)$ y que $f(x+2)$ puede encontrarse mediante divisiones sintéticas repetidas. Así, se tiene

2⌋	3	−2	−5	−1	
		+6	+8	+6	
2⌋	3	+4	+3	+5	$f(2) = 5,$
		+6	+20		
2⌋	3	+10	+23		$f'(2) = 23,$
		+6			
2⌋	3	+16			$f''(2)/2! = 16,\ f'''(2)/3! = 3.$

De aquí que $f(x) = 3x^3 + 16x^2 + 23x + 5$ es el polinomio deseado.

Teorema 18. Un polinomio f(x) *tiene el número* a *como un cero de multiplicidad* m *si y solamente si* $f(a) = 0, f'(a) = 0, \cdots, f^{(m-1)}(a) = 0$ *y* $f^{(m)}(a) \neq 0$.

Si a es un cero de multiplicidad m de $f(x)$, entonces $f(x)$ es divisible entre $(x-a)^m$ y no entre una potencia superior de $x - a$. Escríbase

$$f(x) = f(a) + (x-a)f'(a) + (x-a)^2\frac{f''(a)}{2!} + \cdots + (x-a)^n\frac{f^{(n)}(a)}{n!}$$

De aquí se ve que si a es un cero de multiplicidad m, es necesario que $f(a) = 0, f'(a) = 0, \cdots, f^{(m-1)}(a) = 0$, pero que $f^{(m)}(a) \neq 0$. Recípro-

camente, si $f(a) = 0, f'(a) = 0, \cdots, f^{(m-1)}(a) = 0$, pero si $f^{(m)}(a) \neq 0$, $f(x)$ es divisible, exactamente, entre $(x - a)^m$, pero no entre una potencia superior de $x - a$.

EJERCICIOS

1. Expresar el polinomio $x^3 + 2x - 5$ como un polinomio en $x - 3$ y como un polinomio en $x + 2$.
2. Encontrar un polinomio cada uno de cuyos ceros sea menor en 3 que los ceros de $x^4 - x^3 + 2x - 1$.
3. Encontrar un polinomio cada uno de cuyos ceros sea mayor en 2 que los ceros del polinomio $3x^3 - 4x^2 + 2$.
4. Encontrar un polinomio cada uno de cuyos ceros sea menor en 4 que los ceros del polinomio $3x^4 - 14x^3 + 6x^2 - 9$.
5. Encontrar un polinomio cada uno de cuyos ceros sea mayor en 5 que los ceros del polinomio $2x^3 + 12x^2 + 3$.
6. Demostrar que el polinomio $8x^4 + 84x^3 + 114x^2 + 55x + 9$ tiene un cero de multiplicidad 3.

6 Vectores y matrices

1 · ESPACIOS VECTORIALES

En nuestro estudio de los números complejos se consideraron parejas ordenadas de números reales, (a, b), y se tuvo $(a, b) + (c, d) = (a + c, b + d)$. Además, en álgebra elemental se tiene, $c(a + bi) = ca + (cb)i$ para todo número real c, de modo que es natural definir $c(a, b)$ como igual a (ca, cb). Ahora se considerarán n-adas ordenadas $(x_1, x_2, \cdots, x_n)$, con $x_1, x_2, \cdots, x_n$ elementos de un campo F, y a las n-adas de este tipo se les dará el nombre de *vectores de orden n sobre F*. La *adición* de dos vectores del mismo orden se define por

$$(x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n) = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n),$$

y la *multiplicación por un escalar* por

$$c(x_1, x_2, \cdots, x_n) = (cx_1, cx_2, \cdots, cx_n),$$

cuando c es cualquier elemento de F. Finalmente, $(x_1, x_2, \cdots, x_n) = (y_1, y_2, \cdots, y_n)$ si y solamente si $x_1 = y_1, x_2 = y_2, \cdots, x_n = y_n$; es decir, dos vectores del mismo orden son iguales si y solamente si son idénticos.

La adición y la multiplicación por un escalar de vectores de orden 2 ó 3, sobre el campo de los números reales, pueden representarse geométricamente como se muestra en las figuras de la página 118, para vectores de orden 2.

DEFINICIÓN. Todo conjunto de vectores, sobre un campo F, que es cerrado bajo la adición y la multiplicación por un escalar, recibe el nombre de *espacio vectorial* sobre F.

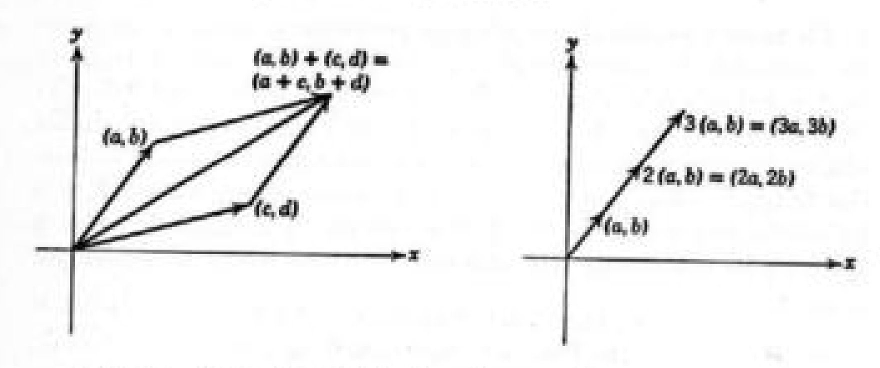
Es evidente que el conjunto de *todos* los vectores de orden n sobre un campo F, constituye un espacio vectorial que se designará por $V_n(F)$. En general, si $\xi_1, \xi_2, \cdots, \xi_m$ son m vectores cualesquiera de $V_n(F)$, el conjunto de todas las *combinaciones lineales*, $c_1\xi_1 + c_2\xi_2 + \cdots + c_m\xi_m$, ($c_1, c_2, \cdots, c_m$ en F) de los vectores $\xi_1, \xi_2, \cdots, \xi_m$, forma un espacio vectorial sobre F. Porque, si $\alpha = a_1\xi_1 + a_2\xi_2 + \cdots + a_m\xi_m$ y $\beta = b_1\xi_1 + b_2\xi_2 + \cdots + b_m\xi_m$, entonces

$$\alpha + \beta = (a_1 + b_1)\xi_1 + (a_2 + b_2)\xi_2 + \cdots + (a_m + b_m)\xi_m$$

y

$$c\alpha = (ca_1)\xi_1 + (ca_2)\xi_2 + \cdots + (ca_m)\xi_m.$$

El espacio vectorial que consiste de todas las combinaciones lineales de un conjunto dado de vectores, recibe el nombre de espacio vectorial *generado* por el conjunto dado de vectores.



EJEMPLO. El espacio vectorial sobre el campo de los números reales, generado por los vectores $(1, 0, 0)$ y $(0, 0, 1)$, es el conjunto de todos los vectores de la forma $(a, 0, b)$, donde a y b son números reales.

La identidad para la adición, en cualquier espacio vectorial que consiste de vectores de orden n, es el vector $(0, 0, \cdots, 0)$ el cual se designará por $\mathbf{0}_n$ o, a menos que pueda existir confusión, simplemente por $\mathbf{0}$. Entonces, evidentemente, el inverso aditivo de $(x_1, x_2, \cdots, x_n)$ es $(-x_1, -x_2, \cdots, -x_n)$ y se deja al estudiante probar que un espacio vectorial forma un grupo abeliano bajo la adición.

Frecuentemente se omite la frase "sobre un campo" cuando se discuten los vectores o los espacios vectoriales. Por supuesto que, en tales casos, el estudiante debe tomar en cuenta que se supone un campo fijo en toda la discusión. Asimismo, cuando se escribe una suma, $\xi + \eta$, se supone que tanto ξ como η son vectores del mismo orden.

Ejercicios

1. Probar que, para todo vector ξ, $0\xi = \mathbf{0}$, $1\xi = \xi$ y $(-1)\xi = -\xi$, donde $-\xi$ es el inverso aditivo de ξ.
2. Probar que $a(b\xi) = (ab)\xi$ para todos los escalares a y b y todos los vectores ξ.
3. Probar que $a(\xi_1 + \xi_2) = a\xi_1 + a\xi_2$ para todos los vectores ξ_1 y ξ_2 y los escalares a.
4. Probar que $(a + b)\xi = a\xi + b\xi$ para todos los escalares a y b y los vectores ξ.
5. Probar que un espacio vectorial forma un grupo abeliano bajo la adición.

2 · DEPENDENCIA E INDEPENDENCIA LINEALES

DEFINICIÓN. Sean $\xi_1, \xi_2, \cdots, \xi_m$ vectores de $V_n(F)$. Si existen elementos $c_1, c_2, \cdots, c_m$ de F, no todos iguales a cero, tales que $c_1\xi_1 + c_2\xi_2 + \cdots + c_m\xi_m = \mathbf{0}$, se dirá que $\xi_1, \xi_2, \cdots, \xi_m$ son *linealmente dependientes*. Si los vectores $\xi_1, \xi_2, \cdots, \xi_m$ no son linealmente dependientes se dirá que son *linealmente independientes*.

EJEMPLO. En $V_3(F)$, donde F es el campo de los números reales, los vectores $(1, -1, 1)$, $(2, 1, -2)$ y $(8, 1, -4)$ son linealmente dependientes, puesto que $2(1, -1, 1) + 3(2, 1, -2) + (-1)(8, 1, -4) = (0, 0, 0)$. Por otra parte, $(1, 0, 0)$, $(0, 1, 0)$ y $(0, 0, 1)$ son linealmente independientes puesto que, si $a(1, 0, 0) + b(0, 1, 0) + c(0, 0, 1) = (a, b, c) = (0, 0, 0)$, entonces $a = b = c = 0$.

Subespacio

Si W es un subconjunto de un espacio vectorial V sobre un campo F de modo que W es asimismo un espacio vectorial sobre F, se dirá que W es un subespacio de V.

EJEMPLO. El conjunto de vectores generado por $(1, 0, 0)$ y $(0, 1, 0)$ es un subespacio de $V_3(F)$.

Teorema 1. Los vectores $\xi_1, \xi_2, \cdots, \xi_m$ sobre un campo **F** *son linealmente dependientes, si y solamente si uno de estos vectores pertenece al subespacio generado por los restantes* $m - 1$.

Porque si $\xi_1, \xi_2, \cdots, \xi_m$ son linealmente dependientes, existen los elementos $c_1, c_2, \cdots, c_m$ de F, no todos cero, tales que

$$c_1\xi_1 + c_2\xi_2 + \cdots + c_m\xi_m = \mathbf{0}.$$

Supóngase que $c_i \neq 0$. Entonces

$$\xi_i = -\frac{c_1}{c_i}\xi_1 - \frac{c_2}{c_i}\xi_2 - \cdots - \frac{c_{i-1}}{c_i}\xi_{i-1} - \frac{c_{i+1}}{c_i}\xi_{i+1} - \cdots - \frac{c_m}{c_i}\xi_m.$$

Por otra parte, si

$$\xi_i = a_1\xi_1 + a_2\xi_2 + \cdots + a_{i-1}\xi_{i-1} + a_{i+1}\xi_{i+1} + \cdots + a_m\xi_m,$$

entonces

$$a_1\xi_1 + a_2\xi_2 + \cdots + a_{i-1}\xi_{i-1} - \xi_i + a_{i+1}\xi_{i+1} + \cdots + a_m\xi_m = 0.$$

Corolario 1. Si los vectores $\xi_1, \xi_2, \cdots, \xi_m$ son linealmente independientes, entonces todo subconjunto de $r < m$ de estos vectores es linealmente independiente.

Corolario 2. Un conjunto de vectores que contiene el vector cero siempre es un conjunto linealmente dependiente.

Las demostraciones de estos corolarios se dejan al estudiante.

Los temas desarrollados en forma detallada, respecto de la dependencia lineal de vectores, se tratan mejor mediante la aplicación de matrices. De aquí que se pospondrán las discusiones adicionales sobre este tópico y se iniciará el estudio de las matrices.

Ejercicios

1. Probar que los vectores (a_1, a_2) y (b_1, b_2) en $V_2(F)$ son linealmente dependientes si y solamente si $a_1b_2 - a_2b_1 = 0$.
2. En $V_3(R)$, donde R es el campo de los números racionales, examinar cada uno de los siguientes conjuntos de vectores respecto de la dependencia lineal.
   a. $(1, 2, 3)$ y $(3, 2, 1)$.
   b. $(8, 4, 8)$ y $(2, 1, 2)$.
   c. $(2, 3, 5)$ y $(4, 9, 25)$.
   d. $(1, 2, 3)$ $(1, 0, 1)$ y $(0, 1, 0)$.
   e. $(1, 2, 0)$, $(0, 3, 1)$ y $(-1, 0, 1)$.
   f. $(-1, 2, 1)$, $(3, 0, -1)$ y $(-5, 4, 3)$.
3. Probar el corolario 1.
4. Probar el corolario 2.

3 · NOTACION MATRICIAL

Al resolver los sistemas de ecuaciones lineales simultáneas, el estudiante pronto se da cuenta que los coeficientes juegan un papel importante para encontrar las soluciones. Las "incógnitas" actúan simplemente como marcas de posición. Por esta razón, se introdujeron nuevas notaciones para simplificar la forma de escribir un sistema de ecuaciones. Por ejemplo, el sistema

$$\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = c_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = c_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n + x_n = c_m \end{array}$$

podría denotarse de la manera siguiente:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \cdot \\ c_m \end{bmatrix}.$$

Aquí se tiene un arreglo rectangular de los a_{ij}, dispuestos en m líneas y n columnas, una columna de n incógnitas x_j y una columna de m constantes c_i. Esta notación nos conduce al estudio de los arreglos rectangulares de elementos llamados matrices. Restringiremos nuestro estudio a las matrices con elementos en un campo.

Definición de matriz

Una matriz A de m por n sobre un campo F es un arreglo rectangular de mn elementos a_{ij} en F dispuestos en m líneas y n columnas, así:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

Se acostumbra encerrar el arreglo con corchetes, paréntesis o una línea recta doble en cada lado del arreglo. Nosotros usaremos la notación indicada arriba. Los elementos $a_{i1}, a_{i2}, \cdots, a_{in}$ son los elementos de la i-ésima línea, mientras que los elementos $a_{1k}, a_{2k}, \cdots, a_{mk}$ son los elementos de la k-ésima columna. Por lo tanto, el primer subíndice indica la línea en la cual se encuentra el elemento, mientras que el segundo subíndice indica la columna. Una sola línea $[a_{i1}\, a_{i2} \cdots a_{in}]$ es asimismo una matriz de 1 por n (o, tal y como escribiremos, de $1 \times n$). Por supuesto que también es un vector de n-ésimo orden, tales vectores recibirán el nombre de *vectores línea*. Por otra parte, una sola columna

$$\begin{bmatrix} a_{1k} \\ a_{2k} \\ \cdot \\ \cdot \\ a_{mk} \end{bmatrix}$$

es una matriz de $m \times 1$, la cual recibirá el nombre de *vector columna.* Frecuentemente, para ahorrar espacio, la matriz A simplemente se escribe

$$[a_{ij}], \quad i = 1, 2, \cdots, m \quad j = 1, 2, \cdots, n.$$

Si $m = n$, la matriz se llama *matriz cuadrada.*

Si se define la *transpuesta*, A^t, de la matriz A, como

$$A^t = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}.$$

se tiene una matriz de $n \times m$ en la cual las líneas son las columnas de A y las columnas son las líneas de A. Entonces, si ξ es un vector columna (una matriz de $m \times 1$), ξ^t es una matriz de $1 \times m$ o sea un vector línea. (Frecuentemente, A^t se denota por A'. Pero, a menudo, se desea usar A' simplemente para referirse a otra matriz y la notación A^t es menos ambigua que A'.)

4 · ADICION Y MULTIPLICACION POR UN ESCALAR

Antes de definir las operaciones con matrices, debe definirse la igualdad de dos matrices. Dos matrices de $m \times n$, $A = [a_{ij}]$ y $B = [b_{ij}]$, son iguales si y solamente si $a_{ij} = b_{ij}$ para todo i y j. En otras palabras, dos matrices son iguales si y solamente si son idénticas.

Suma

La suma $A + B$ de las dos matrices de $m \times n$, A y B, es la matriz de $m \times n$, $C = [c_{ij}]$, donde $c_{ij} = a_{ij} + b_{ij}$. Por lo tanto, para sumar dos matrices de las mismas dimensiones simplemente se suman los elementos en posiciones correspondientes. Obsérvese que la suma de matrices de dimensiones diferentes no está definida y que, cuando las matrices son vectores, la definición coincide con la definición previa de la adición de vectores. Además, como la adición en un campo es conmutativa y asociativa, se ve que la adición de matrices también obedece estas leyes, y que la matriz de $m \times n$ con todos sus elementos iguales a cero es la identidad aditiva para el conjunto de todas las matrices de $m \times n$.

Multiplicación por un escalar

Se define $c[a_{ij}]$, para c en el campo F, como $[ca_{ij}]$ y obsérvese que esto se reduce a la multiplicación por un escalar, de vectores, previamente definida cuando $[a_{ij}]$ es un vector.

Se deja al estudiante la demostración del resultado siguiente.

Teorema 2. Si A *y* B *son matrices de* $m \times n$, *entonces* $(A + B)^t = A^t + B^t$ *y si* c *es un escalar,* $(cA)^t = cA^t$.

Ejercicios

1. Si $A = \begin{bmatrix} 2 & -1 & 0 \\ 1 & 3 & -2 \end{bmatrix}$ y $B = \begin{bmatrix} 3 & -1 & 2 \\ -1 & 0 & 1 \end{bmatrix}$, calcular:

   a. $A + 2B$.
   b. $3A - B$.
   c. $A^t + B^t$.
   d. $(A + B)^t$.

2. Probar el teorema 2.

5 · MULTIPLICACION DE MATRICES

Antes de definir la multiplicación de matrices es conveniente presentar una multiplicación de vectores.

DEFINICIÓN. El *producto interno** de dos vectores $\xi = (x_1, x_2, \cdots, x_n)$ y $\eta = (y_1, y_2, \cdots, y_n)$ es $\xi \cdot \eta = x_1y_1 + x_2y_2 + \cdots + x_ny_n$.

Obsérvese que el producto interno de dos vectores no es un vector sino un escalar. Por ejemplo, $(2, -1) \cdot (3, 4) = 2 \cdot 3 + (-1)4 = 2$.

Ahora, considérese una matriz A de $m \times n$ y una matriz B de $n \times p$ de modo que el número de columnas de A sea igual al número de líneas de B. Puede escribirse A como

(1) $$A = \begin{bmatrix} A_1 \\ A_2 \\ \cdot \\ \cdot \\ \cdot \\ A_m \end{bmatrix},$$

* También llamado *producto punto* o *producto escalar.*

donde A_i es el vector $(a_{i1}, a_{i2}, \cdots, a_{in})$. En forma semejante, puede escribirse B como

(2) $$B = [B_1, B_2, \cdots, B_p],$$

donde $B_k^t = (b_{1k}, b_{2k}, \cdots, b_{nk})$.

DEFINICIÓN. Si A está dada por la ecuación (1) y B por la ecuación (2), entonces AB es la matriz $[c_{ik}]$, donde $c_{ik} = A_i \cdot B_k^t$ para $i = 1, 2, \cdots, n$ y $k = 1, 2, \cdots, p$.

Por lo tanto, AB es una matriz de $n \times p$, en la cual el elemento de la i-ésima línea y k-ésima columna es el producto interno de la i-ésima línea de A por la transpuesta de la k-ésima columna de B.

EJEMPLOS.

1. sea $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ y $B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix}$. entonces

$$AB = \begin{bmatrix} (a_{11}, a_{12}) \cdot (b_{11}, b_{21}) & (a_{11}, a_{12}) \cdot (b_{12}, b_{22}) & (a_{11}, a_{12}) \cdot (b_{13}, b_{23}) \\ (a_{21}, a_{22}) \cdot (b_{11}, b_{21}) & (a_{21}, a_{22}) \cdot (b_{12}, b_{22}) & (a_{21}, a_{22}) \cdot (b_{13}, b_{23}) \end{bmatrix}$$
$$= \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} & a_{11}b_{13} + a_{12}b_{23} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} & a_{21}b_{13} + a_{22}b_{23} \end{bmatrix}.$$

2. sea $A = \begin{bmatrix} 1 & 2 \\ 3 & 1 \\ -1 & 2 \end{bmatrix}$ y $B = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 0 & 1 \end{bmatrix}$. entonces

$$AB = \begin{bmatrix} 1(1) + 2(4) & 1(2) + 2(0) & 1(3) + 2(1) \\ 3(1) + 1(4) & 3(2) + 1(0) & 3(3) + 1(1) \\ (-1)(1) + 2(4) & (-1)(2) + 2(0) & (-1)(3) + 2(1) \end{bmatrix}$$
$$= \begin{bmatrix} 9 & 2 & 5 \\ 7 & 6 & 10 \\ 7 & -2 & -1 \end{bmatrix}.$$

A continuación, se probará que las leyes asociativa y distributiva se cumplen si las matrices consideradas tienen la dimensión apropiada. Para hacerlo, obsérvese que

$$A_i \cdot B_k^t = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk} = \sum_{j=1}^{n} a_{ij}b_{jk}.$$

Así, $AB = [c_{ik}]$, donde

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}.$$

Ley asociativa para la multiplicación

Sea $A = [a_{ij}]$, con $i = 1, 2, \cdots, m$ y con $j = 1, 2, \cdots, n$; sea $B = [b_{jk}]$, con $k = 1, 2, \cdots, p$, y sea $C = [c_{kr}]$, con $r = 1, 2, \cdots, q$. Entonces $AB = [d_{ik}]$, donde $d_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}$, y $(AB)C = [e_{ir}]$ donde $e_{ir} = \sum_{k=1}^{p} d_{ik}c_{kr} = \sum_{k=1}^{p}\sum_{j=1}^{n} a_{ij}b_{jk}c_{kr}$.

Ahora, $BC = [f_{jr}]$, donde $f_{jr} = \sum_{k=1}^{p} b_{jk}c_{kr}$, y $A(BC) = [g_{ir}]$, donde $g_{ir} = \sum_{j=1}^{n} a_{ij}f_{jr} = \sum_{j=1}^{n} a_{ij} \sum_{k=1}^{p} b_{jk}c_{kr} = \sum_{j=1}^{n}\sum_{k=1}^{p} a_{ij}b_{jk}c_{kr} = e_{ir}$. Las sumas pueden intercambiarse porque son sumas en un campo.

Leyes distributivas

Sean A y B las matrices anteriores y $C = [c_{jk}]$, con $j = 1, 2, \cdots, n$ y con $k = 1, 2, \cdots, p$. Se probará que $A(B + C) = AB + AC$. Nótese que, si B es una matriz de $n \times p$, C también debe ser una matriz de $n \times p$ para que pueda realizarse la adición. Ahora, $B + C = [b_{jk} + c_{jk}] = [g_{jk}]$ y $A(B + C) = [h_{ik}]$, donde $h_{ik} = \sum_{j=1}^{n} a_{ij}g_{jk} = \sum_{j=1}^{n} a_{ij}(b_{jk} + c_{jk}) = \sum_{j=1}^{n} a_{ij}b_{jk} + \sum_{j=1}^{n} a_{ij}c_{jk} = d_{ik} + s_{ik}$. Pero $[d_{ik}] = AB$ y $[s_{ik}] = AC$. Por lo tanto, $A(B + C) = AB + AC$. Se deja al estudiante el probar la segunda ley distributiva $(B + C)A = BA + CA$, donde, por supuesto, las matrices deben escogerse con las dimensiones apropiadas.

En general, si tanto A como B son matrices de $m \times m$, no se tiene $AB = BA$. Así,

$$\begin{bmatrix} 1 & -1 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -2 \\ -2 & -2 \end{bmatrix},$$

pero

$$\begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} -3 & 1 \\ 2 & 0 \end{bmatrix}.$$

Sin embargo, si $A = [a_{ij}]$ es una matriz de $m \times m$ con $a_{ij} = 0$ para $i \neq j$, $a_{ii} = a$ para $i = 1, 2, \cdots, m$, y B es otra matriz cualquiera de $m \times m$, es fácil ver que $AB = BA = aB$. Una matriz A de este tipo se llama matriz *escalar*. Si $a = 1$ se tiene la matriz *identidad* I_m de $m \times m$, con la propiedad de que $I_mB = BI_m = B$.

Teorema 3. Si A *es una matriz de* m $\times$ n *y* B *es una matriz de* n $\times$ r, *entonces* $(AB)^t = B^tA^t$.

Sea $A = [a_{ij}]$ y $B = [b_{jk}]$, donde $i = 1, 2, \cdots, m$, $j = 1, 2, \cdots, n$ y $k = 1, 2, \cdots, r$.

Entonces $AB = [c_{ij}]$, donde

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Ahora,

$$B^t = \begin{bmatrix} b_{11} & b_{21} & \cdots & b_{n1} \\ b_{12} & b_{22} & \cdots & b_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ b_{1r} & b_{2r} & \cdots & b_{nr} \end{bmatrix}, \qquad A^t = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}.$$

De aquí que si $B^tA^t = [d_{ij}]$, se tiene

$$d_{ij} = (b_{1i}, b_{2i}, \cdots, b_{ni}) \cdot (a_{j1}, a_{j2}, \cdots, a_{jn}) = \sum_{k=1}^{n} b_{ki} a_{jk}$$

puesto que

$$(a_{j1}, a_{j2}, \cdots, a_{jn}) \cdot (b_{1i}, b_{2i}, \cdots, b_{ni}) = \sum_{k=1}^{n} a_{jk} b_{ki}$$

es el elemento en la j-ésima línea y la i-ésima columna de AB, se sigue que $B^tA^t = (AB)^t$ ya que

$$d_{ij} = \sum_{k=1}^{n} b_{ki} a_{jk} = \sum_{k=1}^{n} a_{jk} b_{ki}.$$

Ejercicios

a. $\begin{bmatrix} 1 & 2 & -1 \\ 3 & 2 & 4 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 3 & -1 \\ 0 & 0 \end{bmatrix}$; b. $[1 \quad 2 \quad 3] \begin{bmatrix} 2 & -1 & 4 \\ 0 & 1 & 5 \\ 2 & 3 & 0 \end{bmatrix}$.

2. Si $A = \begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix}$ $B = \begin{bmatrix} 1 & 3 & 0 \\ 2 & 0 & 1 \end{bmatrix}$, y $C = \begin{bmatrix} 2 \\ 3 \\ -1 \end{bmatrix}$ comprobar haciendo el cálculo correspondiente que $(AB)C = A(BC)$.

3 Si $A = \begin{bmatrix} 2 & -1 \\ 0 & 1 \end{bmatrix}$ y $B = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}$, demostrar que $(A + B)(A + B) = A^2 + AB + BA + B^2 \neq A^2 + 2AB + B^2$.

4. Si $A = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$, encontrar A^2, A^3, A^4.

5. Si $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ y $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, encontrar AB, A^2, B^2, B^2A, y $2A + 3B$.

6. Si $A = [a_{ij}]$ es una matriz de 4×3 y si $B = [b_{jk}]$ es una matriz de 3×4, encontrar el elemento de la tercera línea y segunda columna de AB.

7. Si las dimensiones de las matrices A, B, C se escogen correctamente, probar que $(A + B) + C = A + (B + C)$.
8. Si las dimensiones de las matrices A, B, C se escogen correctamente, probar que $(B + C)A = BA + CA$.
9. Sea $B = [b_{ij}]$ una matriz de $m \times n$ y sea A la matriz de $n \times n$ $[a_{jk}]$, con con $a_{jj} = a$ y con $a_{jk} = 0$ cuando $j \neq k$. Probar que $BA = Ba$.
10. Sean ξ y η vectores de orden n. Probar que $a(\xi \cdot \eta) = (a\xi) \cdot \eta = \xi \cdot (a\eta)$ para todos los escalares a.

6 · MULTIPLICACION DE MATRICES Y TRANSFORMACIONES LINEALES

Regresemos al sistema de ecuaciones dado en la pág. 120. Ahora que se ha definido la multiplicación de matrices se ve que el sistema de ecuaciones puede escribirse $AX^t = C^t$, si se denota la matriz de $m \times n$ por A, la matriz $[x_1, x_2 \cdots, x_n]$ por X y la matriz $[c_1, c_2, \cdots, c_m]$ por C.

Considérese el conjunto de ecuaciones

(3)
$$x' = x \cos \theta_1 - y \operatorname{sen} \theta_1,$$
$$y' = x \operatorname{sen} \theta_1 + y \cos \theta_1.$$

Estas ecuaciones pueden considerarse como la transformación del punto (x, y) en el plano al punto (x', y') en el plano. El punto (x', y') se obtiene a partir del punto (x, y) mediante la rotación del plano alrededor del origen del sistema coordenado en un ángulo θ_1, efectuando la rotación en sentido contrario al movimiento de las manecillas del reloj cuando $\theta_1 > 0$ y en el sentido del movimiento de las manecillas del reloj cuando $\theta_1 < 0$. Este conjunto de ecuaciones también se da mediante la ecuación matricial

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos \theta_1 & -\operatorname{sen} \theta_1 \\ \operatorname{sen} \theta_1 & \cos \theta_1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix},$$

la cual se abreviará como $X' = AX$. Supóngase ahora que se desea hacer una segunda rotación del plano en sentido contrario al movimiento de las manecillas del reloj y en un ángulo θ_2. Esta rotación llevará al punto (x', y') a un tercer punto (x'', y'') y la relación entre las coordenadas está dada por

(4)
$$x'' = x' \cos \theta_2 - y' \operatorname{sen} \theta_2,$$
$$y'' = x' \operatorname{sen} \theta_2 + y' \cos \theta_2.$$

Es geométricamente obvio que estas dos rotaciones realizadas sucesivamente llevan al punto (x, y) al punto (x'', y''). Las relaciones entre las coordenadas x, y y las coordenadas x'', y'' son

$$(5) \qquad \begin{aligned} x'' &= x\cos(\theta_1 + \theta_2) - y\,\mathrm{sen}\,(\theta_1 + \theta_2), \\ y'' &= x\,\mathrm{sen}\,(\theta_1 + \theta_2) + y\cos(\theta_1 + \theta_2). \end{aligned}$$

Se ve que las ecuaciones (5) pueden obtenerse eliminando x' y y' a partir de las ecuaciones (3) y (4). Esta eliminación se efectúa más fácilmente escribiendo las ecuaciones (3) y (4) en forma matricial, así: $X' = AX, X'' = BX'$. Entonces, se ve fácilmente que $X'' = BX' = B(AX) = (BA)X$. El estudiante debe comprobar que, si las ecuaciones (5) se escriben en la forma matricial $X'' = CX$, la matriz $C = BA$.

En general, si el conjunto de m ecuaciones lineales

$$\begin{aligned} x_1' &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n, \\ x_2' &= a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ x_m' &= a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{aligned}$$

expresa las m variables x_i' como funciones lineales de las n variables x_j y si un segundo conjunto de p ecuaciones lineales

$$\begin{aligned} x_1'' &= b_{11}x_1' + b_{12}x_2' + \cdots + b_{1m}x_m', \\ x_2'' &= b_{21}x_1' + b_{22}x_2' + \cdots + b_{2m}x_m', \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ x_p'' &= b_{p1}x_1' + b_{p2}x_2' + \cdots + b_{pm}x_m' \end{aligned}$$

expresa las p variables x_k como funciones lineales de las m variables x_i', entonces, las variables x_k'' pueden expresarse como funciones lineales de las variables x_j. Este cálculo puede hacerse más fácilmente por medio de matrices. Sea $A = [a_{ij}]$, con $i = 1, 2, \cdots, m$ y $j = 1, 2, \cdots, n$; $B = [b_{ki}]$, con $k = 1, 2, \cdots, p$ e $i = 1, 2, \cdots, m$; $X^t = [x_1, x_2, \cdots, x_n]$; $(X')^t = [x_1', x_2', \cdots, x_m']$; $(X'')^t = [x_1'', x_2'', \cdots, x_p'']$. Entonces, los dos sistemas anteriores pueden escribirse como $X' = AX$ y $X'' = BX'$. Así, $X'' = BX' = B(AX) = (BA)X$ y se tiene el resultado deseado. En esta forma el estudiante puede darse cuenta del porqué se ha definido la multiplicación de matrices de la manera particular que se hizo.

Ejercicios

1. Dado $x_1' = 2x_1 - 3x_2$, $x_2' = x_1 + x_2$, $x_1'' = 3x_1' - 4x_2'$ y $x_2'' = x_1' - x_2'$, expresar las variables x_1'' y x_2'' como funciones lineales de x_1 y x_2. Hacer el cálculo por medio de matrices y escribir el resultado final como un sistema de ecuaciones.
2. Dado $x_1' = x_1 - x_2 + x_3$, $x_2' = x_1 + x_3$, $x_1'' = 2x_1' + x_2'$ y $x_2'' = 3x_1' - x_2'$, expresar las variables x_1'' y x_2'' como funciones lineales de x_1, x_2 y x_3. Hacer el cálculo por medio de matrices y escribir el resultado final como un sistema de ecuaciones.

7 · PARTICION DE MATRICES

Sea $A = [a_{ij}]$ una matriz de $m \times n$. El arreglo de elementos de $r \times s$, obtenido a partir de A, eliminando $m - r$ líneas cualesquiera y $n - s$ columnas cualesquiera de A, se llama *submatriz* de A. La matriz A puede partirse en submatrices en muchas formas diferentes. Por ejemplo, la matriz A puede partirse como sigue:

$$A = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix},$$

donde

$$A_1 = \begin{bmatrix} a_{11} & \cdots & a_{1s} \\ \cdots & \cdots & \cdots \\ a_{r1} & \cdots & a_{rs} \end{bmatrix}, \qquad A_2 = \begin{bmatrix} a_{1,s+1} & \cdots & a_{1n} \\ \cdots & & \cdots \\ a_{r,s+1} & \cdots & a_{rn} \end{bmatrix},$$

$$A_3 = \begin{bmatrix} a_{r+1,1} & \cdots & a_{r+1,s} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{ms} \end{bmatrix}, \qquad A_4 = \begin{bmatrix} a_{r+1,s+1} & \cdots & a_{r+1,n} \\ \cdots & \cdots & \cdots \\ a_{m,s+1} & \cdots & a_{mn} \end{bmatrix}.$$

Aquí, A_1 es una matriz de $r \times s$, A_2 es una matriz de $r \times (n - s)$, A_3 una matriz de $(m - r) \times s$ y A_4 una matriz de $(m - r) \times (n - s)$. En ocasiones, para facilitar la multiplicación de dos matrices, es útil partir ambas matrices de manera que la multiplicación puede realizarse usando submatrices. Así, si se desea obtener la matriz AB, donde $B = [b_{jk}]$ es una matriz de $n \times p$, podría ser útil partir A como se indica anteriormente. Entonces, B debe partirse de manera que sea posible efectuar la multiplicación de submatrices. Por ejemplo, B puede partirse de manera que se transforme en un matriz de 2×1 cuyos elementos sean las submatrices B_1 y B_2, así: $B = \begin{vmatrix} B_1 \\ B_2 \end{vmatrix}$, donde B_1 es una matriz de

$s \times p$ y B_2 una matriz de $(n-s) \times p$. Con esta partición se lleva a cabo la multiplicación AB usando como elementos las submatrices A_i y B_i. Por lo tanto, $AB = \begin{bmatrix} A_1B_1 + A_2B_2 \\ A_3B_1 + A_4B_2 \end{bmatrix}$, una matriz de 2×1 con matrices como elementos. Por supuesto que es necesario probar que este producto realmente es igual al producto AB, antes definido, cuando se aplica la regla de la multiplicación por elementos. Ilustraremos la prueba. Por ejemplo, el elemento en la r-ésima línea y la t-ésima columna de AB es $\sum_{j=1}^{n} a_{rj}b_{jt}$, por definición. Además, es el elemento en la r-ésima línea y la t-ésima columna de $A_1B_1 + A_2B_2$, porque puede escribirse este elemento como $\sum_{j=1}^{s} a_{rj}b_{jt} + \sum_{j=s+1}^{n} a_{rj}b_{jt}$. En forma semejante, cualquier otro elemento de AB puede escribirse de manera que se vea que pertenece a una de las dos submatrices de AB.

EJEMPLO

Sea

$$A = \left[\begin{array}{cc:cc} 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & -1 \end{array}\right] = [A_1 \quad A_2]$$

y

$$B = \left[\begin{array}{cc} 1 & 2 \\ 3 & 4 \\ \hdashline 1 & 0 \\ 0 & 1 \end{array}\right] = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix},$$

en las cuales se denota la partición por las líneas punteadas. Entonces $AB = [A_1B_1 + A_2B_2] = [0 + A_2B_2] = [A_2B_2] = \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}$.

8 · EQUIVALENCIA RESPECTO DE LAS LINEAS

El estudiante recordará que el primer método que aprendió para resolver sistemas de ecuaciones lineales simultáneas fue el método de eliminación. Así, para resolver el sistema de ecuaciones,

$$(6) \qquad \begin{aligned} 3x - y &= 6, \\ x + 2y &= 2 \end{aligned}$$

el estudiante podría multiplicar la primera ecuación por 2, sumar la segunda ecuación a la primera, obteniendo $7x = 14$ y, a continuación, dividir entre 7, obteniendo finalmente la ecuación $x = 2$ en lugar de la primera ecuación. Podría ahora sustituir la segunda ecuación con una que se encontrara restando $x = 2$ de la segunda ecuación, obteniendo $2y = 0$ y, finalmente, $y = 0$. Por lo tanto, el proceso para resolver (6) fue encontrar el par más sencillo de ecuaciones $x = 2, y = 0$. Por supuesto que es necesario probar que los valores de x y y, dados al final, satisfacen las ecuaciones originales y que no existen otros valores de x y y que satisfagan el par original. Este tema referente a la equivalencia de los dos conjuntos de ecuaciones se discutirá posteriormente.

Ahora, se dirigirá la atención del estudiante hacia la manipulación esencial relacionada con el método. Obsérvese que, si las ecuaciones (6) se escriben en forma matricial

$$(7) \qquad \begin{bmatrix} 3 & -1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 6 \\ 2 \end{bmatrix}$$

las operaciones realizadas sobre las ecuaciones (6) son esencialmente operaciones realizadas sobre las líneas de las matrices $\begin{bmatrix} 3 & -1 \\ 1 & 2 \end{bmatrix}$ y $\begin{bmatrix} 6 \\ 2 \end{bmatrix}$. La primera ecuación por 2, reemplaza la ecuación (7) por

$$(8) \qquad \begin{bmatrix} 6 & -2 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 12 \\ 2 \end{bmatrix}$$

La segunda operación, a saber, la adición de la segunda ecuación de (6) a la primera ecuación de (6), reemplaza la ecuación matricial (8) por

$$(9) \qquad \begin{bmatrix} 7 & 0 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 14 \\ 2 \end{bmatrix}$$

Continuando en esta forma, sucesivamente se obtiene

$$\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \end{bmatrix},$$

y $$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}2\\0\end{bmatrix}.$$

Efectuando la multiplicación de matrices de la última ecuación matricial, se tiene $\begin{bmatrix}y\\x\end{bmatrix}=\begin{bmatrix}2\\0\end{bmatrix}$, que nos da las dos ecuaciones lineales finales.

Estas operaciones sobre las líneas de una matriz nos conducen a hacernos la pregunta: ¿cuál es la forma, exactamente, que toma una matriz al final si se efectúan tales operaciones sobre sus líneas? Esta pregunta nos lleva hacia una definición más precisa de estas operaciones sobre las líneas.

Operaciones elementales sobre las líneas

Sea $A=[a_{ij}]$ una matriz de $m\times n$. Denotemos la i-ésima línea de A por A_i. Las operaciones elementales sobre las líneas en la matriz A son:

1. El intercambio de dos líneas cualesquiera; es decir, la línea A_k de A puede sustituirse por la línea A_j de A y la línea A_j por A_k.
2. La multiplicación de una línea por un elemento $c\neq 0$ del campo; es decir, la línea A_k puede sustituirse por la línea cA_k, si $c\neq 0$.
3. La adición de una línea a otra; es decir, la línea A_k puede sustituirse por la línea A_j+A_k.

DEFINICIÓN. Se dice que una matriz B de $m\times n$ es *equivalente respecto de las líneas* a una matriz A de $m\times n$, si B puede obtenerse de A mediante un número finito de operaciones elementales sobre las líneas. Se escribe $B\cong A$.

Se ve fácilmente que la equivalencia respecto de las líneas es una verdadera relación de equivalencia. Es obvio que A es equivalente respecto de las líneas a A, porque puede considerarse que A se ha obtenido de A aplicando la operación sobre las líneas (2) con $c=1$, el elemento unidad del campo. Además, si B es equivalente respecto de las líneas a A, A es equivalente respecto de las líneas a B. Porque si B ha sido obtenida a partir de A, mediante la operación elemental sobre las líneas (1), la misma operación elemental sobre las líneas efectuada en B daría A; si B ha sido obtenida de A por la operación sobre las líneas (2), A podría obtenerse de B aplicando una operación sobre las líneas semejante con c sustituido por $1/c$; finalmente, si B ha sido obtenida de A por la operación sobre las líneas (3), A podría obtenerse de B sumando la j-ésima línea multiplicada por -1 a la k-ésima línea. Así, cada operación elemental sobre las líneas tiene una inversa que es una operación elemental sobre las líneas o una combinación de operaciones elementales sobre las líneas. Finalmente, la propiedad transitiva es obvia, porque si B puede obtenerse partiendo de A y si C puede obtenerse partiendo de B, entonces C puede obtenerse de A mediante operaciones elementales sobre las líneas.

Matriz en forma de escalón

Se dice que una matriz está en forma de escalón * si: (a) todas las líneas diferentes de cero (si existen) preceden a las líneas cero; (b) si en cada línea sucesiva diferente de cero, el número de ceros que preceden al primer elemento diferente de cero, es mayor que el número de ceros en la línea precedente, y (c) el primer elemento diferente de cero (si existe) en una línea es 1.

EJEMPLOS. Las matrices

$$\begin{bmatrix}0 & 1 & 2 & 3\\0 & 0 & 1 & -1\\0 & 0 & 0 & 0\end{bmatrix} \quad y \quad \begin{bmatrix}1 & 3 & 0 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}$$

están en forma de escalón. Las matrices

$$\begin{bmatrix}0 & 0 & 2 & 1\\0 & 3 & 1 & 4\\0 & 0 & 0 & 0\end{bmatrix} \quad y \quad \begin{bmatrix}0 & 1 & 2\\0 & 0 & -1\\0 & 0 & 3\end{bmatrix}$$

no están en forma de escalón

Se dice que una matriz se encuentra en forma de escalón *reducida* si está en forma de escalón y, cuando el primer elemento diferente de cero de la i-ésima línea se encuentra en la j-ésima columna, todos los demás elementos de la j-ésima columna son cero. Por lo tanto, la primera matriz en forma de escalón, de los ejemplos anteriores, no está en forma de escalón reducida mientras que la segunda sí lo está.

Teorema 4. Una matriz de m × n *es equivalente respecto de las líneas a una matriz de* m × n *en forma de escalón reducida.*

Es posible que todo elemento de la primera columna de la matriz dada A sea cero, o existe un elemento x que no sea cero en la k-ésima

* Se encuentran varias definiciones de la forma de escalón en textos diferentes. En particular, algunos autores no exigen la condición (c).

línea, digamos, de esta columna. En el último caso, intercámbiese la primera y la k-ésima líneas de A. Entonces, x aparece en la primera línea y la primera columna de la matriz resultante y puede sustituirse por 1 multiplicando la primera línea de la matriz por x^{-1}. Entonces, los elementos restantes de la primera columna pueden hacerse cero sumando los múltiplos apropiados de la primera línea a las otras líneas. Así, A es equivalente respecto de las líneas a una matriz en cualquiera de las formas $[0 \quad C]$ o $\begin{bmatrix} 1 & D \\ 0 & E \end{bmatrix}$, donde, en el primer caso, 0 representa la matriz cero de $m \times 1$ y C una matriz de $m \times (n-1)$, mientras que, en el segundo caso, 0 representa la matriz cero de $(m-1) \times 1$, D una matriz de $1 \times (n-1)$ y E una matriz de $(m-1) \times (n-1)$. En el primer caso se repite el proceso anterior con la matriz C, mientras que en el segundo caso se repite el proceso con la matriz E. Si en el último caso, E ha sido reemplazada por una matriz con 1 en la primera línea y primera columna, puede sumarse un múltiplo apropiado de esta línea a la primera línea de la martiz completa para hacer el primer elemento de D igual a cero, sin cambiar la primera columna de la matriz completa. Por lo tanto, en todos los casos, continuando el proceso se llega a la forma deseada.

Matrices elementales

Una matriz de $m \times m$, obtenida a partir de la matriz identidad I de $m \times m$ por medio de una operación elemental sobre las líneas de I, se llama matriz elemental. Por tanto, existen tres tipos de matrices elementales correspondientes a las tres operaciones elementales sobre las líneas. A continuación, se describirán estos tipos. Denotemos la i-ésima línea de una matriz A por A_i. Sean P, Q y R las matrices obtenidas de I efectuando en I las operaciones elementales sobre las líneas (1), (2) y (3), respectivamente. Entonces, estas matrices elementales puede describirse del modo siguiente:

$$P \text{ con } P_i = I_i, \quad i \neq j, k, \quad P_j = I_k, \quad P_k = I_j;$$
$$Q \text{ con } Q_i = I_i, \quad i \neq k, \quad Q_k = cI_k, \quad c \neq 0;$$
$$R \text{ con } R_i = I_i, \quad i \neq k, \quad R_k = I_j + I_k.$$

EJEMPLOS

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}; \quad Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$
$$j = 2, k = 3. \qquad k = 2. \qquad j = 3, k = 2.$$

Teorema 5. Cada una de las operaciones elementales sobre las líneas en una matriz A *de* m $\times$ n, *puede efectuarse mediante la premultiplicación de* A *por una matriz elemental.*

Para intercambiar la j-ésima y la k-ésima líneas de A se forma el producto PA. Denotemos por $[PA]_i$ la i-ésima línea de PA. Recuérdese que la i-ésima línea de PA se obtiene tomando el producto interno de la i-ésima línea de P con la transpuesta de cada columna de A que corresponda. Así, $[PA]_i = P_iA = I_iA = A_i$ cuando $i \neq j, k$; $[PA]_j = P_jA = I_kA = A_k$, y $[PA]_k = P_kA = I_jA = A_j$. El estudiante puede comprobar fácilmente que la matriz QA es la matriz obtenida de A por medio de la operación sobre las líneas (2). En forma semejante, RA es la matriz obtenida de A efectuando la operación sobre las líneas (3) en A, puesto que se tiene $[RA]_i = R_iA = I_iA = A_i$ cuando $i \neq [RA]_k = R_kA = (I_j + I_k)A = I_jA + I_kA = A_j + A_k$.

Corolario. Si una matriz B *de* m $\times$ n *es equivalente respecto de las líneas a una matriz* A *de* m $\times$ n, *entonces* B = SA, *donde* S *es un producto de matrices elementales.*

Ejercicios

1. Encontrar las matrices en forma de escalón reducida equivalentes, respecto de las líneas, a:

a. $\begin{bmatrix} 1 & 2 & -1 & 4 \\ 3 & 2 & 0 & 2 \\ 0 & 1 & 3 & 2 \\ 3 & 3 & 3 & 4 \end{bmatrix}$; b. $\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ -1 & 2 \\ 1 & 1 \end{bmatrix}$; c. $\begin{bmatrix} 0 & -1 & 3 \\ 2 & -4 & 1 \\ 0 & 3 & 2 \end{bmatrix}$.

2. Sea I la matriz identidad de $m \times m$ y A una matriz de $m \times n$. Probar que (a) $I_iA = A_i$ y (b) $(I_j + I_k)A = A_j + A_k$.

3. Dada la matriz $A = \begin{bmatrix} 2 & -1 & 4 \\ 3 & 5 & 6 \end{bmatrix}$. En cada uno de los casos siguientes exhibir la matriz E tal que EA sea, (*a*) la matriz obtenida de A intercambiando las dos líneas; (*b*) la matriz obtenida de A dividiendo la segunda línea entre 2; (*c*) la matriz obtenida de A sumando la primera línea a la segunda.

4. Si $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 2 & 1 \end{bmatrix}$, exhibir la matriz elemental E tal que $EA = \begin{bmatrix} 2 & 1 \\ 0 & 1 \\ 1 & 2 \end{bmatrix}$ y la matriz elemental F tal que $FA = \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 2 & 2 \end{bmatrix}$.

5. Si $A = \begin{bmatrix} 1 & 3 & -1 \\ 2 & 2 & 0 \end{bmatrix}$, exhibir el producto de las matrices elementales que la reduce a una matriz equivalente respecto de las líneas en forma de escalón reducida.
6. Demostrar que $\begin{bmatrix} 1 & 2 & 1 \\ 3 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix}$ es equivalente respecto de las líneas a la matriz identidad de 3×3.

9 · MATRICES NO SINGULARES

DEFINICIÓN. Se dice que una matriz cuadrada A es *no singular* si existe una matriz B tal que $BA = AB = I$. Si B existe, se denotará por A^{-1} y se llamará *inversa* de A. Si A^{-1} no existe, se dice que la matriz A es *singular*.

Teorema 6. La inversa de una matriz no singular es única.

Sea $BA = AB = I$ y $CA = AC = I$. Entonces $BA = CA$, $(BA)B = (CA)B$, $B(AB) = C(AB)$, $BI = CI$ y $B = C$.

Teorema 7. Si A *y* B *son matrices no singulares, entonces el producto* AB *es una matriz no singular. Además,* $(AB)^{-1} = B^{-1}A^{-1}$.

Ahora, B^{-1} y A^{-1} existen. De aquí que $(B^{-1}A^{-1})(AB) = B^{-1}[A^{-1}(AB)] = B^{-1}[(A^{-1}A)B] = B^{-1}(IB) = B^{-1}B = I$. En forma semejante, $(AB)(B^{-1}A^{-1}) = I$. Así, AB es no singular y $B^{-1}A^{-1}$ es su inversa.

Teorema 8. Las matrices elementales P, Q *y* R *son no singulares.*

Puesto que $PP = I$, P es su propia inversa. Las matrices Q^{-1} y R^{-1} se describen presentando sus líneas: $Q_i^{-1} = I_i$ cuando $i \neq k$ y $Q_k^{-1} = c^{-1}I_k$; $R_i^{-1} = I_i$ cuando $i \neq k$ y $R_k^{-1} = I_k - I_j$.

Puesto que el producto de matrices no singulares es no singular, un producto de matrices elementales es no singular. De aquí que el corolario del teorema 5 se transforma en

Teorema 9. Si una matriz B *es equivalente respecto de las líneas a una matriz* A, *entonces* B = SA, *donde* S *es no singular.*

Teorema 10. Una matriz A *de* n × n *es equivalente respecto de las líneas a la matriz identidad si y solamente si es no singular.*

Primero, sea A no singular. Encontrar una matriz B en forma de escalón reducida equivalente respecto de las líneas a A. Entonces, $B = SA$, donde S es una matriz no singular. De aquí que B es no singular porque el producto de matrices no singulares es no singular y B^{-1} existe. Ahora, se demostrará que B no puede tener un cero en su diagonal principal; es decir, si el elemento en la i-ésima línea y la j-ésima columna de B se denota por b_{ij}, entonces $b_{kk} \neq 0$ para todo k. Recuérdese que, por lo menos, $j - 1$ ceros preceden al primer elemento diferente de cero en la j-ésima línea de B. De aquí que, si $b_{kk} = 0$, la $(k+1)$-ésima línea de B tiene, por lo menos, $k + 1$ ceros precediendo su primer elemento diferente de cero. Si $k = n$, la n-ésima línea de B consiste de ceros y si $k < n$, por lo menos una línea de B después de la k-ésima consiste de ceros. En consecuencia, si $b_{kk} = 0$, B tiene una línea de ceros. Entonces, $BB^{-1} = I$ tiene una línea de ceros, contrario a la definición de I. Por lo tanto, $b_{ii} = 1$ y $b_{ij} = 0$ cuando $i \neq j$. En consecuencia, B es la matriz identidad y de aquí que A es equivalente respecto de las líneas a la matriz identidad.

Segundo, sea A equivalente respecto de las líneas a la matriz identidad I. Entonces $I = SA$, donde S es no singular y de aquí que $A = S^{-1}I$ es no singular.

Teorema 11. Si una matriz cuadrada se reduce a la matriz identidad por una sucesión de operaciones sobre las líneas, la misma sucesión de operaciones sobre las líneas efectuada sobre la identidad produce la inversa de la matriz dada.

Sea A la matriz dada y denotemos por E_i las matrices elementales. (Nótese que aquí no estamos usando la notación para una línea de una matriz). Ahora, se da $(E_s \cdots E_2E_1)A = I$. De aquí que $(E_s \cdots E_2E_1) \cdot (AA^{-1}) = IA^{-1}$, dando $(E_s \cdots E_2E_1)I = A^{-1}$, el resultado deseado.

EJEMPLO. Encontrar la inversa de la matriz $A = \begin{bmatrix} 1 & -2 \\ 1 & 1 \end{bmatrix}$. Ahora, efectuando una operación sobre las líneas cada vez, se presentan las matrices equivalentes respecto de las líneas a A, en la columna de la izquierda y las matrices sucesivas equivalentes respecto de las líneas a I, en la columna de la derecha:

$$\begin{bmatrix} 0 & -3 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} -\frac{1}{3} & \frac{1}{3} \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -\frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{3} & \frac{2}{3} \\ -\frac{1}{3} & \frac{1}{3} \end{bmatrix} = A^{-1}.$$

Combinando los resultados de los tres teoremas precedentes, ahora se tienen los dos corolarios siguientes.

Corolario 1. Una matriz es no singular si y solamente si puede escribirse como un producto de matrices elementales.

Corolario 2. Una matriz B *es equivalente respecto de las líneas a una matriz* A *si y solamente si* B = SA, *donde* S *es una matriz no singular.*

Ejercicios

1. Probar: Si A es una matriz no singular, entonces su transpuesta, A^t, es una matriz no singular.
2. Encontrar las inversas de las matrices siguientes sobre el campo de los números racionales y sobre el campo de las clases de residuos módulo 5:

$$\text{a. } \begin{bmatrix} 1 & -3 & 2 \\ 2 & 0 & 0 \\ 1 & 4 & 1 \end{bmatrix}; \quad \text{b. } \begin{bmatrix} 2 & 4 & 3 \\ 0 & 1 & 1 \\ 2 & 2 & -1 \end{bmatrix}; \quad \text{c. } \begin{bmatrix} 1 & 2 & -2 \\ -1 & 3 & 0 \\ 0 & -2 & 1 \end{bmatrix}.$$

3. Encontrar la inversa de la matriz sobre el campo de los números complejos:

$$\begin{bmatrix} i & -1 & 2i \\ 2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix}.$$

4. ¿Tiene la matriz siguiente una inversa sobre el campo de los números racionales?

$$\begin{bmatrix} 2 & 1 & 3 & 1 \\ 1 & 2 & -1 & 4 \\ 3 & 3 & 2 & 5 \\ 1 & -1 & 4 & -3 \end{bmatrix}.$$

5. Probar el corolario 1 y el corolario 2.
6. Probar que la matriz $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ es no singular si y solamente si $ad - bc \neq 0$.
7. Si A es una matriz de $n \times n$ tal que $A^2 - A + I$ es la matriz cero, probar que A es no singular y que $A^{-1} = I - A$.
8. Probar que el conjunto de todas las matrices no singulares de $n \times n$ forman un grupo respecto de la multiplicación de matrices.

10 · EQUIVALENCIA RESPECTO DE LAS COLUMNAS

Si en la definición de una operación elemental sobre las líneas, la palabra línea se cambia por la palabra columna, se tiene la definición de una operación elemental sobre las columnas en una matriz. En forma semejante, la definición de la equivalencia de dos matrices respecto de las columnas, puede leerse de la definición de la equivalencia de dos matrices respecto de las columnas, reemplazando la palabra línea por la palabra columna. Una operación elemental sobre las columnas, en una matriz A, se transforma en una operación elemental sobre las líneas en la transpuesta, A^t, de A. Considérese que B se obtiene de A por una operación elemental sobre las columnas. Entonces B^t puede obtenerse de A^t por una operación elemental sobre las líneas. Por lo tanto, $B^t = EA^t$, donde E es una matriz elemental y, en consecuencia, $B = AE^t$. De aquí, se tiene el teorema siguiente:

Teorema 12. Una operación elemental sobre las columnas en una matriz A *de* m × n *puede efectuarse multiplicando* A *por la derecha por una matriz de* n × n, *obtenida de la matriz identidad de* n × n *por la misma operación elemental sobre las columnas.*

En forma semejante, si B es equivalente respecto de las columnas a una matriz A, B^t es equivalente respecto de las líneas a A^t, $B^t = SA^t$ y $B = AS^t$, donde S^t es no singular. Recíprocamente, si $B = AT$, donde T es no singular, $B^t = T^tA^t$, de modo que B^t es equivalente respecto de las líneas a A^t y, en consecuencia, B es equivalente respecto de las columnas a A. De aquí, se tiene el teorema siguiente.

Teorema 13. Una matriz B *de* m × n *es equivalente respecto de las columnas a una matriz* A *de* m × n *si y solamente si* B = AT, *donde* T *es una matriz no singular de* n × n.

11 · EQUIVALENCIA DE MATRICES

Ahora, ambas operaciones sobre líneas y sobre columnas pueden aplicarse a una matriz. Si una matriz B de $m \times n$ puede obtenerse de una matriz A de $m \times n$, por medio de un número finito de operaciones elementales sobre líneas y sobre columnas, se dice que la matriz B es *equivalente* a la matriz A. Por lo tanto, la equivalencia respecto de las

líneas y respecto de las columnas son casos especiales del concepto general de la equivalencia de matrices. Combinando los resultados anteriores, se tiene el teorema siguiente que se usa frecuentemente como una definición de la equivalencia de dos matrices.

Teorema 14. Una matriz B *de* m × n *es equivalente a una matriz de* m × n *si y solamente si* $B = SAT$, *donde* S *y* T *son matrices no singulares de* m × m *y* n × n, *respectivamente.*

Teorema 15. Forma canónica. Toda matriz A, *diferente de cero, de* m × n *es equivalente a una matriz de* m × n *de la forma* $\begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$ *donde* I *es la matriz identidad de* r × r *y donde las submatrices restantes son matrices cero.*

Sea a algún elemento de A diferente de cero. Efectuando operaciones elementales sobre líneas y columnas en A, se obtiene una matriz equivalente con el elemento a en la primera línea y la primera columna. Multiplíquese la primera línea de esta matriz por a^{-1}. Entonces, restando múltiplos adecuados de la primera línea, de las líneas restantes, y múltiplos adecuados de la primera columna, de las columnas restantes, se obtiene una matriz equivalente de la forma $B = \begin{bmatrix} 1 & 0 \\ 0 & C \end{bmatrix}$, donde C es una submatriz de $(m-1) \times (n-1)$ y donde las otras submatrices son la matriz identidad de 1×1 y las matrices cero de $1 \times (n-1)$ y $(m-1) \times 1$. Ahora, puede establecerse la forma canónica por inducción sobre m. Si $m = 1$, entonces B está en forma canónica. Supóngase que el teorema es verdadero para todas las matrices de $(m-1) \times (n-1)$. De aquí que la submatriz C de B es equivalente a una matriz en forma canónica. En consecuencia, B es equivalente a una matriz en forma canónica porque las operaciones sobre las líneas y sobre las columnas, efectuadas sobre C para obtener D, pueden efectuarse sobre las últimas $m-1$ líneas y las últimas $n-1$ columnas de B.

En el teorema 5 del capítulo siguiente se probará que la forma canónica de una matriz es única.

Ejercicios

1. Dada la matriz $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \end{bmatrix}$, encontrar las matrices no singulares T y U tales que $AT = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 0 & 2 \end{bmatrix}$ y $AU = \begin{bmatrix} 1 & 2 & 5 \\ 0 & 1 & 3 \end{bmatrix}$.

2. Encontrar las formas canónicas de las matrices del ejercicio 1, pág. 135 y del ejercicio 4, pág. 138.
3. Aplicando el teorema 14 como la definición de equivalencia de dos matrices, probar que la equivalencia de las matrices es una verdadera relación de equivalencia; es decir, demostrar que es simétrica, reflexiva y transitiva.

12 · CRITERIOS PARA LA DEPENDENCIA LINEAL DE VECTORES

Regresemos al problema de determinar si un conjunto dado de vectores $\xi_1, \xi_2, \cdots, \xi_m$ de $V_n(F)$ es o no un conjunto de vectores linealmente dependiente. Se dirá que una combinación lineal $c_1\xi_1 + c_2\xi_2 + \cdots + c_m\xi_m$ es una combinación lineal *no trivial* si, por lo menos, uno de los $c_1, c_2, \cdots, c_m$ es diferente de cero. Si $c_1 = c_2 = \cdots = c_m = 0$ se dirá que la combinación lineal es una combinación *trivial.*

Teorema 16. Sean $\xi_1, \xi_2, \cdots, \xi_m$ *vectores de* $V_n(F)$ *y sean* a *y* b *escalares con* $b \neq 0$. *Entonces, cada combinación lineal no trivial de* $\xi_1, \xi_2, \cdots, \xi_m$ *es una combinación no trivial de* $\xi_1, \xi_2, \cdots, \xi_{j-1}, a\xi_i + b\xi_j, \xi_{j+1}, \cdots, \xi_m$ *y, recíprocamente, cada combinación lineal no trivial de* $\xi_1, \xi_2, \cdots, \xi_{j-1}, a\xi_i + b\xi_j, \xi_{j+1}, \cdots, \xi_m$ *es una combinación no trivial de* $\xi_1, \xi_2, \cdots, \xi_m$.

Se tiene

$$\begin{aligned} c_1\xi_1 + c_2\xi_2 + \cdots + c_m\xi_m = {} & c_1\xi_1 + c_2\xi_2 + \cdots + c_{i-1}\xi_{i-1} \\ & + \left(c_i - \frac{c_j a}{b}\right)\xi_i + c_{i+1}\xi_{i+1} + \cdots + c_{j-1}\xi_j \\ & + \frac{c_j}{b}(a\xi_i + b\xi_j) + c_{j+1}\xi_{j+1} + \cdots + c_m\xi_m. \end{aligned}$$

Si

$$\begin{aligned} c_1 = c_2 = \cdots = c_{i-1} = c_i - \frac{c_j a}{b} = c_{i+1} = \cdots = c_{j-1} = \frac{c_j}{b} \\ = c_{j+1} = \cdots = c_m = 0, \end{aligned}$$

entonces $c_j = 0$, de modo que $c_i = 0$. De aquí que $c_1 = c_2 = \cdots = c_m = 0$.

Inversamente, se tiene

$$\begin{aligned} c_1\xi_1 + c_2\xi_2 + \cdots + c_{j-1}\xi_j + c_j(a\xi_i + b\xi_j) + c_{j+1}\xi_{j+1} \\ + \cdots + c_m\xi_m = c_1\xi_1 + c_2\xi_2 + \cdots + c_{i-1}\xi_{i-1} \\ + (c_i + ac_j)\xi_i + c_{i+1}\xi_{i+1} + \cdots + (bc_j)\xi_j \\ + c_{j+1}\xi_{j+1} + \cdots + c_m\xi_m. \end{aligned}$$

Si

$$c_1 = c_2 = \cdots = c_{i-1} = c_i + ac_j = c_{i+1} = \cdots = bc_j$$
$$= c_{j+1} = \cdots = c_m = 0,$$

entonces $bc_j = 0$, $c_j = 0$ y $c_i = 0$. De aquí que $c_1 = c_2 = \cdots, = c_m = 0$.

Teorema 17. Si un conjunto de vectores diferentes de cero $\xi_1, \xi_2, \cdots \xi_m$ *en* $V_n(F)$ *es linealmente dependiente sobre* F, *entonces existe un subconjunto máximo de* $r < m$ *vectores que es linealmente independiente sobre* F. *Los restantes* $m - r$ *vectores son combinaciones lineales de los* r *linealmente independientes.*

Escogemos algún vector $\xi_j \neq 0$. Entonces ξ_j es linealmente independiente sobre F puesto que $c\xi_j = 0$ implica $c = 0$. Ahora, si $\xi_1, \xi_2, \cdots, \xi_{j-1}, \xi_{j+1}, \cdots, \xi_m$ todos son múltiplos escalares de ξ_j, se ha demostrado. Si no, existe un vector $\xi_k (k \neq j)$ que no es un múltiplo escalar de ξ_j. Ahora, se tienen dos vectores, ξ_j y ξ_k, linealmente independientes. Si los restantes $m - 2$ vectores todos son combinaciones lineales de ξ_j y ξ_k, se ha completado la demostración. Si no, se tiene un vector $\xi_i (i \neq j, i \neq k)$ que no es una combinación lineal de ξ_j y ξ_k. Se continúa en esta forma hasta que se tiene un conjunto de $r(< m)$ vectores linealmente independientes tales que los restantes $m - r$ vectores son combinaciones lineales de estos r vectores.

En cada paso de este proceso debe escogerse un vector ξ_j, ξ_k, ξ_i, etc., y ahora debemos hacernos la pregunta de si diferentes selecciones de vectores en varios pasos conduciría a un número máximo mayor de vectores linealmente independientes. Supóngase, entonces, que primero se ha escogido un conjunto de vectores linealmente independientes $\eta_1, \eta_2, \cdots, \eta_r$, donde cada $\eta_i (i = 1, 2, \cdots, r)$ es uno de los $\xi_j (j = 1, 2, \cdots, m)$ y cada uno de los restantes $m - r$ vectores entre los $\xi_1, \xi_2, \cdots, \xi_m$ es una combinación lineal de los $\eta_1, \eta_2, \cdots, \eta_r$. Ahora, supóngase que también se ha seleccionado un conjunto de vectores linealmente independientes $\zeta_1, \zeta_2, \cdots, \zeta_s$, donde cada $\zeta_i (i = 1, 2, \cdots, s)$ es uno de los $\xi_j (j = 1, 2, \cdots, m)$ y cada uno de los $m - s$ vectores restantes entre los $\xi_1, \xi_2, \cdots, \xi_m$ es una combinación lineal de $\zeta_1, \zeta_2, \cdots, \zeta_s$.

Supóngase que $s \geqq r$. Ahora, afirmamos que, por lo menos, uno de los vectores $\eta_i (i = 1, 2, \cdots, r)$ es una combinación lineal $b_1\zeta_1 + b_2\zeta_2 + \cdots + b_s\zeta_s$, de los ζ_i con $b_1 \neq 0$. Porque cada vector ξ_j es una combinación lineal de los η_i y, si cada η_i puede expresarse como una combinación lineal de los $\zeta_2, \zeta_3, \cdots, \zeta_s$, cada vector ξ_j puede expresarse como una combinación lineal de los $\zeta_2, \zeta_3, \cdots, \zeta_s$. En particular, ζ_1 (siendo uno de los ξ_j) puede expresarse así, contrario a la independencia lineal de los $\zeta_1, \zeta_2, \cdots, \zeta_s$.

Numerando otra vez los vectores, si es necesario, ahora puede suponerse que $\eta_1 = b_1\zeta_1 + b_2\zeta_2 + \cdots + b_s\zeta_s$ con $b_1 \neq 0$. Y puede afirmarse que $\eta_1, \zeta_2, \zeta_3, \cdots, \zeta_s$ forman un conjunto linealmente independiente de vectores tales que los restantes $m - s$ vectores del conjunto $\xi_1, \xi_2, \cdots, \xi_m$ son combinaciones lineales de los $\eta_1, \zeta_2, \zeta_3, \cdots, \zeta_s$. Porque si $\xi_j = a_1\zeta_1 + a_2\zeta_2 + \cdots + a_s\zeta_s$, se tiene $\zeta_1 = (1/b_1)(\eta_1 - b_2\zeta_2 - \cdots - b_s\zeta_s)$ y de aquí que $\xi_j = (a_1/b_1)\eta_1 + (a_2 - b_2/b_1)\zeta_2 + \cdots + (a_s - b_s/b_1)\zeta_s$. Además, si $c_1\eta_1 + c_2\zeta_2 + c_3\zeta_3 + \cdots + c_s\zeta_s = 0$, se tiene $c_1b_1\zeta_1 + (c_1b_2 + c_2)\zeta_2 + (c_1b_3 + c_3)\zeta_3 + \cdots + (c_1b_s + c_s)\zeta_s = 0$. Puesto que $\zeta_1, \zeta_2, \cdots, \zeta_s$ son linealmente independientes, $c_1b_1 = 0$. Pero $b_1 \neq 0$, de modo que $c_1 = 0$ y de aquí que $c_2 = c_3 = \cdots = 0$ y los $\eta_1, \zeta_2, \zeta_3, \cdots, \zeta_s$ son linealmente independientes.

Ahora, por lo menos uno de los vectores $\eta_2, \eta_3, \cdots, \eta_r$ es una combinación lineal $b_1\eta_1 + b_2\zeta_2 + b_3\zeta_3 + \cdots + b_s\zeta_s$, con $b_2 \neq 0$. Porque precisamente se ha demostrado que todo vector de los vectores $\xi_1, \xi_2, \cdots, \xi_m$ es una combinación lineal de ese tipo. De aquí que, si cada uno de los $\eta_i (i = 2, 3, \cdots, r)$ puede expresarse como una combinación lineal de los $\eta_1, \zeta_3, \zeta_4, \cdots \zeta_s$, todo vector ξ_j puede expresarse como una combinación lineal de los $\eta_1, \zeta_3, \zeta_4, \cdots, \zeta_s$. Entonces, en particular, ζ_2 puede expresarse así, lo que es contrario a la independencia lineal de los $\eta_1, \zeta_2, \zeta_3, \cdots, \zeta_s$.

Numeramos otra vez los vectores, si es necesario, de manera que $\eta_2 = b_1\eta_1 + b_2\zeta_2 + b_3\zeta_3 + \cdots + b_s\zeta_s$ con $b_2 \neq 0$ y puede demostrarse, tal y como se hizo en los párrafos anteriores, que ahora los $\eta_1, \eta_2, \zeta_3, \zeta_4, \cdots, \zeta_s$ forman un conjunto de vectores linealmente independientes tales que los restantes $m - s$ vectores del conjunto $\xi_1, \xi_2, \cdots, \xi_m$ son combinaciones lineales de los $\eta_1, \eta_2, \zeta_3, \zeta_4, \cdots, \zeta_s$.

Continuando, se obtiene el conjunto linealmente independiente $\eta_1, \eta_2, \cdots, \eta_r, \zeta_{r+1}, \cdots, \zeta_s$, de manera que, de acuerdo con la propiedad máxima de $\eta_1, \eta_2, \cdots, \eta_r$, se tiene $s = r$.

De acuerdo con los teoremas 16 y 17 y la definición de matrices equivalentes, es evidente que, si B es una matriz equivalente a A, los vectores línea de A son linealmente dependientes si y solamente si los vectores línea de B son linealmente dependientes. Además, es obvio que los vectores línea diferentes de cero, de una matriz en forma de escalón, son linealmente independientes. Por ejemplo, si se tiene la matriz

$$\begin{bmatrix} 1 & 2 & -1 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

en forma de escalón y se tiene $c_1(1, 2, -1, 2) + c_2(0, 0, 1, 1) + c_3(0, 0, 0, 1) = (0, 0, 0, 0)$, debe tenerse $c_1 = c_2 = c_3 = 0$. Nótese que, al aplicar este criterio, se obtienen los mismos resultados si los primeros elementos diferentes de cero, de cada línea, simplemente son números cualesquiera diferentes de cero y no necesariamente todos 1. Así, se ve que los vectores $(2, 0, -1)$ y $(0, 3, 1)$ son linealmente independientes al examinar la matriz

$$\begin{bmatrix} 2 & 0 & -1 \\ 0 & 3 & 1 \end{bmatrix}.$$

De aquí que, para determinar si un conjunto dado de m vectores es linealmente dependiente o no, se colocan los vectores como líneas de una matriz y se lleva esta matriz a su forma de escalón (sin importar que los primeros elementos, diferentes de cero, de cada línea, sean necesariamente 1). Entonces, el conjunto dado de vectores es linealmente dependiente si y solamente si, por lo menos, una de las líneas, en esta forma de escalón, es una línea cero. Además, si existen r líneas diferentes de cero, entonces r es el número máximo de los m vectores que son linealmente independientes sobre F.

Ejercicios

1. Examinar los siguientes conjuntos de vectores respecto de la dependencia lineal sobre el campo de los números racionales. Si los vectores son linealmente dependientes, encontrar el número máximo de vectores del conjunto que son linealmente independientes.

   a. $(1, 3, -2), (2, 2, 6), (3, -2, 5)$.
   b. $(1, 0, 1), (0, 2, 2), (3, 7, 1)$.
   c. $(-2, 4, 6), (5, 7, -3), (1, 15, 9)$.
   d. $(1, -1, 1, 3), (2, -5, 3, 10), (3, 3, 1, 2)$.
   e. $(1, 6, -2, 5), (4, 0, 4, -2), (7, 2, 0, 2), (-6, 3, -3, 3)$.
   f. $(2, 4, 3, -1, -2, 1), (2, 2, 4, 2, 6, 2), (0, -1, 0, 3, 6, 1)$.

2. ¿Son linealmente independientes los vectores $(1, 1, 0), (1, 0, 1), (0, 1, 1)$ sobre el campo de los enteros módulo 2? ¿Sobre el campo de los enteros módulo 3?
3. Se dice que un conjunto de vectores $\xi_1, \xi_2, \cdots, \xi_m$ es un conjunto *mutuamente ortogonal* si $\xi_i \cdot \xi_j = 0$ para $i, j = 1, \cdots, m$ e $i \neq j$. Probar que cualquier conjunto de vectores, diferentes de cero, mutuamente ortogonales, es linealmente independiente.

4. Probar que un conjunto de vectores ξ_1 y ξ_2 es un conjunto linealmente dependiente si y solamente si uno de estos vectores es igual a un escalar multiplicado por el otro.

7 Sistemas de ecuaciones lineales

1 · RANGO DE UNA MATRIZ

Rango línea de una matriz

El número máximo r de líneas linealmente independientes, sobre un campo F, de una matriz de $m \times n$ se llama rango línea de la matriz.

Teorema 1. Las matrices equivalentes a las líneas tienen el mismo rango línea.

Sean A y B dos matrices de $m \times n$ equivalentes respecto a las líneas. Considérense los vectores línea $\xi_1, \xi_2, \cdots, \xi_m$ de A y $\eta_1, \eta_2, \cdots, \eta_m$ de B. Ahora, A y B tienen el mismo rango línea si y solamente si el número máximo de los vectores $\xi_1, \xi_2, \cdots, \xi_m$, que son linealmente independientes, es igual al número máximo de los vectores $\eta_1, \eta_2, \cdots, \eta_m$ que son linealmente independientes. Ahora, puesto que A y B son matrices equivalentes respecto a las líneas, $\eta_1, \eta_2, \cdots, \eta_m$ pueden obtenerse de $\xi_1, \xi_2, \cdots, \xi_m$ mediante una sucesión de las operaciones siguientes: (a) el intercambio de ξ_i y ξ_k; (b) la multiplicación de algún ξ_j por un elemento $b \neq 0$ del campo, y (c) la sustitución de ξ_j por $\xi_i + \xi_j$.

Es obvio que el conjunto obtenido de $\xi_1, \xi_2, \cdots, \xi_m$ por la aplicación de (a), tiene el mismo número máximo de vectores linealmente independientes. De acuerdo con el teorema 16 del capítulo 6, se ve que el número máximo de vectores linealmente independientes no cambia por la aplicación de (b) (tómese $a = 0$ en el teorema 16) o por la aplicación de (c) (tómese $a = b = 1$ en el teorema 16).

Corolario 1. Si una matriz A *tiene el rango línea* r, *entonces* SA, *donde* S *es una matriz no singular, tiene el rango línea* r.

Este hecho es obvio si se recuerda que SA es una matriz equivalente a A respecto a las líneas.

Corolario 2. El rango línea de una matriz no singular de n $\times$ n *es* n.

Simplemente se necesita recordar que una matriz no singular es equivalente a la matriz identidad respecto a las líneas y es obvio que las líneas de la matriz identidad son linealmente independientes.

Rango columna de una matriz

El rango columna de una matriz es el número máximo de columnas linealmente independientes de la matriz. Es obvio que los teoremas anteriores sobre el rango línea de una matriz pueden transformarse en los teoremas correspondientes sobre el rango columna de una matriz. Así se tienen los dos teoremas siguientes.

Teorema 2. Las matrices equivalentes respecto a las columnas tienen el mismo rango columna.

Teorema 3. Si T *es una matriz no singular, la matriz* A *y la matriz* AT *tienen el mismo rango columna.*

Teorema 4. El rango línea de una matriz es igual a su rango columna.

Sea A cualquier matriz diferente de cero. Existen las matrices no singulares S y T tales que $SAT = C$ es una matriz en forma canónica. El rango línea y el rango columna de C son iguales a r, la dimensión de la submatriz identidad de C. El rango línea de A y SA es el mismo, digamos r_1. Por lo tanto, el rango línea de $CT^{-1} = SA$ es r_1. Pero CT^{-1} tiene cuando más r líneas diferentes de cero puesto que si $T^{-1} = \begin{bmatrix} T_1 \\ T_2 \end{bmatrix}$, $CT^{-1} = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} T_1 \\ T_2 \end{bmatrix} = \begin{bmatrix} IT_1 \\ 0 \end{bmatrix} = \begin{bmatrix} T_1 \\ 0 \end{bmatrix}$, donde T_1 es una matriz de r líneas. Puesto que T^{-1} es no singular, sus líneas son linealmente independientes y, por tanto, las líneas de T_1 son linealmente independientes. De aquí que CT^{-1} es de rango línea r y $r_1 = r$. Ahora, considérese la transpuesta $T^tA^tS^t = C^t$. Los rangos línea de T^tA^t y A^t son los mismos. Así, como antes, el rango línea de $T^tA^t = C^t(S^t)^{-1}$ es r y de aquí que el rango columna de AT y, por lo tanto, el de A es r.

En consecuencia, el término de rango de una matriz puede significar el rango línea o el rango columna.

Teorema 5. La forma canónica de una matriz es única.

En el teorema precedente se demostró que el rango de A es igual al rango de C. Si, ahora, existen las matrices no singulares S_1 y T_1 tales que $S_1AT_1 = C_1$, una forma canónica diferente de C, el rango de A es igual al rango de C_1. De aquí que los rangos de C y C_1 son iguales y, por lo tanto, las matrices C y C_1 son idénticas.

Puede establecerse en otra forma nuestro trabajo anterior sobre dependencia e independencia lineal de los conjuntos de vectores en los teoremas siguientes.

Teorema 6. Dos matrices de m $\times$ n *son equivalentes si y solamente si tienen el mismo rango.*

Teorema 7. El rango de una matriz en forma de escalón es igual al número de sus líneas diferentes de cero.

Ejercicios

1. ¿Son equivalentes los siguientes pares de matrices? ¿Por qué?

a. $\begin{bmatrix} 2 & -1 & 3 & 4 \\ 0 & 3 & 4 & 1 \\ 2 & 3 & 7 & 5 \\ 2 & 5 & 11 & 6 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & -5 & 6 \\ 3 & -2 & 1 & 2 \\ 5 & -2 & -9 & 14 \\ 4 & -2 & -4 & 8 \end{bmatrix}$.

b. $\begin{bmatrix} 4 & -1 & 2 \\ 3 & 4 & 0 \\ 1 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 2 & 1 & 4 & 7 \\ 3 & 6 & 2 & 1 \\ 0 & 0 & 1 & 5 \end{bmatrix}$.

2. Determinar el rango de cada una de las matrices siguientes para valores racionales del parámetro k:

a. $\begin{bmatrix} 2 & 1 & -1 & 2 \\ 1 & 1 & 0 & 1 \\ k & 3 & -2 & 0 \\ 0 & 1 & -4 & 4 \end{bmatrix}$. b. $\begin{bmatrix} k & 1 & 1 \\ 1 & k & 1 \\ 1 & 1 & k \end{bmatrix}$.

c. $\begin{bmatrix} 1 & 1 & -1 & 2 \\ k & 1 & 1 & 1 \\ 1 & -1 & 3 & -3 \\ 4 & 2 & 0 & k \end{bmatrix}$.

3. ¿Son linealmente dependientes o linealmente independientes sobre F, las m líneas de una matriz de $m \times n$ sobre un campo F cuando $m > n$? ¿Por qué?

2 · ECUACIONES LINEALES SIMULTANEAS SOBRE UN CAMPO

A continuación, se aplicará la teoría de las matrices, desarrolada en los párrafos anteriores, a la resolución de m ecuaciones lineales simultáneas con n incógnitas $x_1, x_2, \cdots, x_n$, con coeficientes y términos constantes sobre un campo F. Escribiremos el sistema de ecuaciones

$$
(1) \qquad \begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= c_1,\\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= c_2,\\
\cdots\cdots\cdots\cdots\cdots\cdots&\cdots\cdots\\
a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= c_m
\end{aligned}
$$

en la forma matricial $AX = C$, donde A es la matriz de $m \times n[a_{ij}]$, $X^t = [x_1, x_2, \cdots, x_n]$ y $C^t = [c_1, c_2, \cdots, c_m]$. La matriz A se llama *matriz de los coeficientes* del sistema de ecuaciones. El caso más sencillo de resolver, es aquel en el que el número de ecuaciones es igual al número de incógnitas y la matriz de los coeficientes es no singular.

Teorema 8. La ecuación AX = C, *con* m = n *y* A *no singular, tiene la solución única* $X = A^{-1}C$.

Puesto que A es no singular, la multiplicación de $AX = C$ por A^{-1} da $X = A^{-1}C$. Sustituyendo este resultado en $AX = C$, se tiene $A(A^{-1}C) = IC = C$.

Veamos ahora el caso en que no se restringe la relación entre el número de incógnitas y el número de ecuaciones. Aquí se necesita considerar los rangos de la matriz de los coeficientes y el de la matriz *aumentada* $A^* = [AC]$, la cual es una matriz de $m \times (n+1)$ que se obtiene al agregar a A la columna de constantes $c_i, i = 1, 2, \cdots, m$. Se observa que el rango de A^* siempre es mayor que o igual al rango de A, porque A^* tiene, por lo menos, tantas columnas linealmente independientes como A.

En el siguiente lema se muestra la relación entre las soluciones de la ecuación $AX = C$ y las de la ecuación $SAX = SC$, donde S es una matriz no singular. Obsérvese que la premultiplicación por la matriz no singular S es equivalente a efectuar operaciones sobre las líneas en A y C o efectuar estas operaciones en las ecuaciones lineales (1).

Lema. Si existe una solución $x_1', x_2', \cdots, x_n'$ *de la ecuación* AX = C, *entonces también es una solución de la ecuación* SAX = SC, *donde* S *es una matriz no singular. Recíprocamente, si* $x_1', x_2', \cdots, x_n'$ *es una solución de la ecuación* SAX = SC, *donde* S *es no singular, es una solución de la ecuación* AX = C.

Sea X', donde $(X')^t = [x_1', x_2', \cdots, x_n']$, una solución de $AX = C$; es decir, $AX' = C$ es una identidad. Entonces, obviamente, $SAX' = SC$ es una identidad. Recíprocamente, si X' es una solución de $SAX = SC$, es decir, si $SAX' = SC$ es una identidad, entonces $S^{-1}(SAX') = S^{-1}(SC)$ nos da la identidad $AX' = C$. Así se ha demostrado que todas las soluciones de $AX = C$ son soluciones de $SAX = SC$ y que no se tienen soluciones diferentes a las originales para la ecuación $AX = C$, cuando se multiplica por una matriz no singular.

DEFINICIÓN. Si el sistema de ecuaciones (1) tiene una solución, se dice que las ecuaciones son *consistentes*. Si el sistema no tiene solución, se dice que las ecuaciones son *inconsistentes*.

Teorema 9. La ecuación AX = C *tiene una solución si y solamente si el rango de* A, *la matriz de los coeficientes, es igual al rango de la matriz aumentada* A*. *Si* A *y* A* *tienen el mismo rango, denotaremos por* r *su rango común. Entonces,* r *de las incógnitas pueden expresarse como funciones lineales de las constantes* c_i *y a las restantes* n − r *incógnitas pueden asignárseles valores arbitrarios.*

Sea A de rango r. Transfórmese A a una matriz escalón reducida equivalente respecto a las líneas. Solamente las primeras r líneas contienen elementos diferentes de cero. Considérese que los primeros elementos diferentes de cero, en estas r líneas, se encuentran en las columnas $k_1, k_2, \cdots, k_r$, respectivamente. Estas operaciones sobre las líneas en A pueden efectuarse premultiplicando por una matriz no singular S. Multiplíquese cada miembro de la ecuación $AX = C$ por S, obteniendo $SAX = SC$. Ahora, las últimas $m - r$ líneas de SA están compuestas de ceros y de aquí que las últimas $m - r$ líneas de SAX están compuestas de ceros. Por lo tanto, si la ecuación $AX = C$ es consistente, las últimas $m - r$ líneas de SC están necesariamente compuestas de ceros. Ahora, considérese que las últimas $m - r$ líneas de SC están compuestas de ceros y sean $b_1, b_2, \cdots, b_r$ los elementos diferentes de cero de SC. Además, denotemos por p_{ij} el elemento que se encuentra en la i-ésima línea y la j-ésima columna de SA. Entonces, la ecuación matricial $SAX = SC$ proporciona el siguiente conjunto de r ecuaciones:

$$
\begin{aligned}
x_{k_1} + p_{1,k_1+1}x_{k_1+1} + \cdots + p_{1n}x_n &= b_1,\\
x_{k_2} + p_{2,k_2+1}x_{k_2+1} + \cdots + p_{2n}x_n &= b_2,\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
x_{k_r} + p_{r,k_r+1}x_{k_r+1} + \cdots + p_{rn}x_n &= b_r
\end{aligned}
$$

donde $p_{1,k_j} = 0$ para $j = 2, 3, \cdots, r$; $p_{2,k_j} = 0$ para $j = 3, 4, \cdots, r$; $\cdots, p_{r-1,k_j} = 0$ para $j = r$. Así pueden expresarse las $x_{k_1}, x_{k_2}, \cdots, x_{k_r}$ como funciones lineales de las restantes x_j y de las constantes b_i. El lema nos dice que ésta es una solución de la ecuación $AX = C$.

Se tiene que las últimas $m - r$ líneas de SA están compuestas de ceros y que la ecuación $AX = C$ tiene una solución si y solamente si las últimas $m - r$ líneas de SC están compuestas de ceros. De aquí que, si $AX = C$ tiene una solución, SA y SA^* tienen el mismo rango puesto que SA^* es la matriz SA aumentada por la columna de b_i. Así, si $AX = C$ tiene una solución, A y A^* tienen el mismo rango. Recíprocamente, si A y A^* tienen el mismo rango, SA y SA^* también tienen el mismo rango y de aquí que SA^* tiene $m - r$ líneas con ceros y la ecuación $AX = C$ tiene una solución. Por lo tanto, la ecuación $AX = C$ tiene una solución si y solamente si A y A^* tienen el mismo rango.

EJEMPLO. Resolver el siguiente sistema de ecuaciones:

$$
\begin{aligned}
x - y + 2z + w &= 2,\\
3x + 2y + w &= 1,\\
4x + y + 2z + 2w &= 3.
\end{aligned}
$$

Escríbase el sistema en forma matricial

$$
\begin{bmatrix} 1 & -1 & 2 & 1\\ 3 & 2 & 0 & 1\\ 4 & 1 & 2 & 2 \end{bmatrix}
\begin{bmatrix} x\\ y\\ z\\ w \end{bmatrix} = \begin{bmatrix} 2\\ 1\\ 3 \end{bmatrix}
$$

Se transforma A^* a una matriz escalón reducida, transformando simultáneamente a A en una matriz escalón reducida.

$$
A^* = \begin{bmatrix} 1 & -1 & 2 & 1 & 2\\ 3 & 2 & 0 & 1 & 1\\ 4 & 1 & 2 & 2 & 3 \end{bmatrix} \simeq \begin{bmatrix} 1 & 0 & \frac{4}{5} & \frac{3}{5} & 1\\ 0 & 1 & -\frac{6}{5} & -\frac{2}{5} & -1\\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.
$$

Por lo tanto, el rango de ambas matrices, A y A^*, es 2 y de aquí que las ecuaciones son consistentes. La ecuación matricial se transforma en

$$
\begin{bmatrix} 1 & 0 & \frac{4}{5} & \frac{3}{5}\\ 0 & 1 & -\frac{6}{5} & -\frac{2}{5}\\ 0 & 0 & 0 & 0 \end{bmatrix}
\begin{bmatrix} x\\ y\\ z\\ w \end{bmatrix} = \begin{bmatrix} 1\\ -1\\ 0 \end{bmatrix},
$$

dando

$$
\begin{aligned}
x &= -\tfrac{4}{5}z - \tfrac{3}{5}w + 1,\\
y &= \tfrac{6}{5}z + \tfrac{2}{5}w - 1.
\end{aligned}
$$

Cuando estos valores de x y y se sustituyen en las ecuaciones del sistema original, las ecuaciones se reducen a identidades. Pueden darse valores arbitrarios a z y w y, así, este sistema de ecuaciones tiene un número infinito de soluciones.

Ejercicios

Resolver los siguientes sistemas de ecuaciones. Si se introduce un parámetro k, considérense las soluciones para valores racionales de k.

1. $3x - 2y + z + 6 = 0,$
   $2x + 5y - 3z - 2 = 0,$
   $4x - 9y + 5z + 14 = 0.$

2. $4x + 7y - 14z = 10,$
   $2x + 3y - 4z = -4,$
   $x + y + z = 6.$

3. $4x - y + z = 5,$
   $2x - 3y + 5z = 1,$
   $x + y - 2z = 2,$
   $5x - z = 2.$

4. $2x - y - 2z = 0,$
   $x - 2y + z = 0,$
   $2x - 3y - z = 0.$

5. $kx - 3y - 5 = 0,$
   $8x + y - 17 = 0,$
   $kx + 2y - 10 = 0.$

6. $6x + 4y + 3z - 84w = 0,$
   $x + 2y + 3z - 48w = 0,$
   $x - 2y + z - 12w = 0,$
   $4x - 4y - z - 24w = 0.$

7. $x + y - z = 2,$
   $kx + y + z = 1,$
   $x - y + 3z = -3,$
   $4x + 2y = k.$

8. $x + y + 2z = 9,$
   $x + y - z = 0,$
   $2x - y + z = 3,$
   $x + 3y + 2z = 1.$

9. $x + y + 2w = 0,$
   $y + z = 0,$
   $x + z = 0,$
   $x + y + z + w = 0,$
   $x + y + 2z = 0.$

10. $x + ky + 3 = 0,$
    $kx + 3y + 1 = 0,$
    $kx + 4y - 6 = 0.$

11. $2x + y + 3z = 1,$
    $4x + 2y - z = -3,$
    $2kx + y - 4z = -4,$
    $10x + y - 6z = -10.$

12. $2x + y + 3z = 1,$
    $4x + 2y - z = -3,$
    $2kx + y - 4z = -4.$

13. $3x + y - z = 4,$
$kx + y + z = 2,$
$x + y - z = 1,$
$x - z = k.$

14. $2x - y - 3z + 4w = 0,$
$x + 3y + z - w = 0,$
$4x + 5y - 2z + 6w = 0,$
$3x - y - z - 7w = 0.$

3 · ECUACIONES LINEALES HOMOGENEAS

Si en la ecuación matricial $AX = C$ la matriz C es una matriz cero, el sistema de ecuaciones (1) es un conjunto de ecuaciones lineales homogéneas. Se nota que, en este caso, los rangos de la matriz aumentada y de la matriz de los coeficientes son los mismos, de modo que siempre existen soluciones de un conjunto de ecuaciones lineales homogéneas. Además, es obvio que $(0, 0, \cdots, 0)$ siempre es una solución. Entonces, la cuestión interesante es saber cuándo las ecuaciones lineales homogéneas tienen soluciones diferentes a $(0, 0, \cdots, 0)$, la solución trivial.

Teorema 10. Un sistema de m *ecuaciones lineales homogéneas con* n *incógnitas tiene una solución diferente a* $(0, 0, \cdots, 0)$ *si y solamente si el rango de la matriz de los coeficientes es menor que* n.

Este es un corolario obvio del teorema 9. Si el rango de la matriz de los coeficientes es $r < n$, entonces $n - r > 0$ y r de las incógnitas pueden expresarse como funciones lineales de las $n - r > 0$ incógnitas. Si $r = n$, la ecuación $SAX = 0$ muestra que las n incógnitas deben ser todas iguales a cero. Por lo tanto, solamente si $r < n$ existe un número infinito de soluciones diferentes a $(0, 0, \cdots, 0)$.

El caso especial $m = n$ merece que se considere por separado.

Corolario. Un sistema de n *ecuaciones lineales homogéneas con* n *incógnitas tiene una solución diferente a* $(0, 0, \cdots, 0)$ *si y solamente si la matriz de los coeficientes es singular.*

Si la matriz de los coeficientes es singular su rango es menor que n.

Puede ser interesante observar que la solución general de la ecuación $AX = C$ puede expresarse como la suma de la solución general de la ecuación $AX = 0$ más una solución particular de la ecuación $AX = C$, siendo una solución particular de $AX = C$ aquella en la que se dan valores particulares a los parámetros arbitrarios de la solución general. En el ejemplo ilustrativo de la pág. 152 la solución del sistema de ecuaciones homogéneas

$$x - y + 2z + w = 0,$$
$$3x + 2y + w = 0,$$
$$4x + y + 2z + 2w = 0$$

es $x = -(4/5)z - (3/5)w, y = (6/5)z + (2/5)w$. Una solución particular del sistema no homogéneo es $z = 0, w = 0, x = 1, y = -1$.

4 · SOLUCIONES LINEALMENTE INDEPENDIENTES DE SISTEMAS DE ECUACIONES LINEALES

Es interesante determinar el número de soluciones linealmente independientes de un sistema consistente $AX = C$, de m ecuaciones lineales con n incógnitas. Se probará el siguiente teorema.

Teorema 11. Si un sistema de m *ecuaciones lineales no homogéneas con* n *incógnitas tiene una solución, tiene exactamente* n − r + 1 *soluciones linealmente independientes, donde* r *es el rango de la matriz de los coeficientes. Un sistema de* m *ecuaciones lineales homogéneas con* n *incógnitas tiene exactamente* n − r *soluciones linealmente independientes, siendo* r *el rango de la matriz de los coeficientes.*

Sea r el rango de la matriz de los coeficientes y de la matriz aumentada del sistema $AX = C$, de m ecuaciones lineales con n incógnitas. Entonces, las soluciones pueden expresarse de la manera siguiente:

$$x_1 = \sum_{j=r+1}^{n} d_{1j}x_j + b_1,$$

(2)
$$x_2 = \sum_{j=r+1}^{n} d_{2j}x_j + b_2,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$x_r = \sum_{j=r+1}^{n} d_{rj}x_j + b_r.$$

Se observa que si $r = n$, solamente existe la solución $b_1, b_2, \cdots, b_n$. Si las ecuaciones son homogéneas, todas las b son ceros. Por lo tanto, el teorema se cumple para $r = n$. Ahora, supóngase que $r < n$. Se construye una matriz cuyas líneas representen soluciones particulares de la ecuación $AX = C$. Primero, sea $x_j = 0, j = r + 1, \cdots, n$. Entonces, una solución es $x_1 = b_1, x_2 = b_2, \cdots, x_r = b_r, x_j = 0, j = r + 1, \cdots, n$. A continuación, sea $x_k = 1$, con $k \geq r + 1$ y $x_j = 0$, con $k \neq j$ y $j \geq r + 1$. Así se obtienen $n - r + 1$ soluciones. *Sea* $x_1', x_2', \cdots, x_n'$ otra solución cualquiera. La matriz de estas soluciones es una matriz de $(n - r + 2) \times n$.

$$\begin{bmatrix} x_1' & x_2' & \cdots & x_r' & x'_{r+1} & x'_{r+2} & \cdots & x_n' \\ b_1 & b_2 & \cdots & b_r & 0 & 0 & \cdots & 0 \\ d_{1,r+1}+b_1 & d_{2,r+1}+b_2 & \cdots & d_{r,r+1}+b_r & 1 & 0 & \cdots & 0 \\ d_{1,r+2}+b_1 & d_{2,r+2}+b_2 & \cdots & d_{r,r+2}+b_r & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ d_{1n}+b_1 & d_{2n}+b_2 & & d_{rn}+b_r & 0 & 0 & & 1 \end{bmatrix}$$

Nótese que las últimas $n-r$ líneas de esta matriz son linealmente independientes, porque sus últimas $n-r$ columnas forman la matriz identidad $(n-r)\times(n-r)$. Así, el rango columna de esta submatriz de $(n-r)\times n$ es $\geq n-r$, pero su rango columna es $\leq n-r$. De aquí que su rango es $n-r$ tal y como se afirmó. Además, si no todas las b_i son cero, las últimas $n-r+1$ líneas son linealmente independientes, porque estas líneas contienen la submatriz de $(n-r+1)\times(n-r+1)$, que consiste de las últimas $n-r$ columnas y la columna que contiene $b_k \neq 0$, cuyas columnas son linealmente independientes. Así, si no todas las b_i son cero, se ha exhibido un conjunto de $n-r+1$ soluciones linealmente independientes. Si los b_i son todos cero, las ecuaciones son homogéneas porque, de (2), $(0,0,\cdots,0)$ es una solución. En este caso se ha exhibido un conjunto de $n-r$ soluciones linealmente independientes. Falta probar que cualquier otra solución $x_1', x_2', \cdots, x_n'$ es una combinación lineal del conjunto dado. Para hacerlo, denotemos por R_i la i-ésima línea de la matriz de soluciones dada. Entonces,

$$R_1 - \sum_{j=r+1}^{n} x_j'(R_{j-r+2} - R_2) - R_2 = 0,$$

porque es necesario observar que, por hipótesis, solamente $x_1', x_2', \cdots, x_n'$ satisfacen las ecuaciones (2). Así, cualquier solución $x_1', x_2', \cdots, x_n'$ es una combinación lineal del conjunto dado de soluciones linealmente independientes.

EJEMPLO. En el ejemplo de la pág. 152 $n=4$ y $r=2$, de manera que existen 3 soluciones linealmente independientes. Estas pueden tomarse como $x=1$, $y=-1$, $z=0$, $w=0$; $x=1/5$, $y=1/5$, $z=1$, $w=0$ y $x=2/5$, $y=-3/5$, $z=0$, $w=1$.

Ejercicios

1. ¿m ecuaciones lineales homogéneas con n incógnitas tienen soluciones diferentes a $(0,0,\cdots,0)$ cuando $m<n$? ¿Por qué?

2. Exhibir un conjunto máximo de soluciones linealmente independientes para cada uno de los siguientes sistemas de ecuaciones:

a. $2x-3y+4z+w=0,$
$x+z-w=0,$
$3x-3y+5z=0,$
$4x-3y+6z-w=0.$

b. $2x-2y+5z+3w=0,$
$4x-y+z+w=0,$
$3x-2y+3z+4w=0,$
$x-3y+7z+6w=0.$

c. $x+y-z=2,$
$3x+y+z=1,$
$x-y+3z=-3,$
$4x+2y=3.$

d. $2x+3y-4z+5w=2,$
$3x+5y-z+2w=1,$
$7x+11y-9z+12w=5,$
$3x+4y-11z+13w=5.$

3. Sean $\xi_1=(1,2,3)$, $\xi_2=(2,-1,1)$ y $\xi_3=(1,7,8)$. Encontrar los números c_1, c_2, c_3, no todos cero, tales que $c_1\xi_1+c_2\xi_2+c_3\xi_3=0$.
4. Sean $\xi_1=(1,-1,3)$, $\xi_2=(2,3,5)$, $\xi_3=(-1,4,-2)$ y $\xi_4=(4,1,-2)$. Encontrar los números c_1, c_2, c_3 y c_4, no todos cero, tales que $c_1\xi_1+c_2\xi_2+c_3\xi_3+c_4\xi_4=0$.

5 · DIMENSION Y BASE DE UN ESPACIO VECTORIAL

DEFINICIÓN. La *dimensión* de un espacio vectorial V sobre F es igual al número máximo de vectores linealmente independientes en V.

Podría esperarse que la dimensión de $V_n(F)$ sea n. Para establecer este resultado primero se probará un lema.

Lema. Cualquier conjunto de r *vectores de* $V_n(F)$ *es linealmente dependiente si* $r > n$.

Supóngase que los vectores son $\xi_1=(a_{11},a_{21},\cdots,a_{n1})$, $\xi_2=(a_{12},a_{22},\cdots,a_{n2}),\cdots,\xi_r=(a_{1r},a_{2r},\cdots,a_{nr})$. Entonces $\xi_1,\xi_2,\cdots,\xi_r$ son linealmente dependientes si y solamente si existen los escalares $x_1,x_2,\cdots,x_r$, no todos cero, tales que $x_1\xi_1+x_2\xi_2+\cdots+x_r\xi_r=(0,0,\cdots,0)$. Así, $\xi_1,\xi_2,\cdots,\xi_r$ son linealmente dependientes si y solamente si existe una solución no trivial para el sistema de n ecuaciones lineales homogéneas en las r incógnitas:

$$\begin{aligned} x_1a_{11}+x_2a_{12}+\cdots+x_ra_{1r}&=0\\ x_1a_{21}+x_2a_{22}+\cdots+x_ra_{2r}&=0\\ \cdots\cdots\cdots\cdots\cdots&\\ x_1a_{n1}+x_2a_{n2}+\cdots+x_ra_{nr}&=0. \end{aligned}$$

Puesto que el rango de la matriz de los coeficientes de este sistema es $\leq n < r$, se deduce, de acuerdo con el teorema 10, que existe una solución no trivial.

Teorema 12. El espacio vectorial $V_n(F)$ *tiene la dimensión* n.

De acuerdo con el lema, la dimensión de $V_n(F)$ no es mayor que n. Ahora, se observa que los n vectores $\xi_1 = (1, 0, 0, \cdots, 0), \xi_2 = (0, 1, 0, \cdots, 0), \cdots, \xi_n = (0, 0, 0, \cdots, 1)$ son linealmente independientes sobre F puesto que $c_1\xi_1 + c_2\xi_2 + \cdots + c_n\xi_n = (c_1, c_2, \cdots, c_n) = (0, 0, \cdots, 0)$ implica que $c_1 = c_2 = \cdots = c_n = 0$. Por lo tanto, la dimensión de $V_n(F)$ es mayor que o igual a n, y de aquí que la dimensión es n.

Teorema 13. Si el espacio vectorial V *sobre* F *es generado por los* m *vectores* $\xi_1, \xi_2, \cdots, \xi_m$ *y* $r > m$, *entonces todo conjunto de* r *vectores de* V *es linealmente dependiente.*

Sea $\eta_1, \eta_2, \cdots, \eta_r$ cualquier conjunto de r vectores de V. Puesto que $\xi_1, \xi_2, \cdots, \xi_m$ generan V, se sabe que existen los escalares a_{ij} en $F(i = 1, 2, \cdots, m; j = 1, 2, \cdots, r)$ tales que

$$\begin{aligned} \eta_1 &= a_{11}\xi_1 + a_{21}\xi_2 + \cdots + a_{m1}\xi_m \\ \eta_2 &= a_{12}\xi_1 + a_{22}\xi_2 + \cdots + a_{m2}\xi_m \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_r &= a_{1r}\xi_1 + a_{2r}\xi_r + \cdots + a_{mr}\xi_m. \end{aligned}$$

Ahora, debe demostrarse que existen los escalares $x_1, x_2, \cdots, x_r$ de F tales que

$$x_1\eta_1 + x_2\eta_2 + \cdots + x_r\eta_r = 0. \text{ pero}$$

$$\begin{aligned} x_1\eta_1 &+ x_2\eta_2 + \cdots + x_r\eta_r \\ &= (x_1a_{11} + x_2a_{12} + \cdots + x_ra_{1r})\xi_1 + (x_1a_{21} + x_2a_{22} + \cdots + x_ra_{2r})\xi_2 \\ &\quad + \cdots + (x_1a_{m1} + x_2a_{m2} + \cdots + a_{mr})\xi_m. \end{aligned}$$

Por lo tanto, $\eta_1, \eta_2, \cdots, \eta_r$ son linealmente dependientes si existe una solución no trivial del sistema de ecuaciones lineales homogéneas

$$\begin{aligned} x_1a_{11} + x_2a_{12} + \cdots + x_ra_{1r} &= 0 \\ x_1a_{21} + x_2a_{22} + \cdots + x_ra_{2r} &= 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots& \\ x_1a_{m1} + x_2a_{m2} + \cdots + x_ra_{mr} &= 0. \end{aligned}$$

Puesto que $r > m$, se sigue, de acuerdo al teorema 10, que existe esa solución no trivial.

Teorema 14. Sea V *un espacio vectorial de dimensión* m *sobre* F *y supóngase que los vectores* $\xi_1, \xi_2, \cdots, \xi_s$ *generan* V. *Entonces* (1) $s \geq m$; (2) *algunos* m *de los* s *vectores* $\xi_1, \xi_2, \cdots, \xi_s$ *son linealmente independientes, y* (3) *si* $s \geq t > m$, *cualesquiera* t *de los* s *vectores* $\xi_1, \xi_2, \cdots, \xi_s$ *son linealmente dependientes.*

Sea r el número máximo de vectores linealmente independientes que pueden escogerse de entre los vectores $\xi_1, \xi_2, \cdots, \xi_s$. Puesto que pueden numerarse otra vez los vectores, si se desea, no se pierde generalidad si se supone que este conjunto máximo es $\xi_1, \xi_2, \cdots, \xi_r$. Supóngase que $r < s$; entonces, $\xi_1, \xi_2, \cdots, \xi_r$ son linealmente independientes, pero los conjuntos de vectores $\xi_1, \xi_2, \cdots, \xi_r, \xi_{r+j}$ son linealmente dependientes para $j = 1, 2, \cdots, s - r$. De aquí que existen los escalares $c_1, c_2, \cdots, c_r, c_{r+j}$, no todos cero, tales que

$$(3) \qquad c_1\xi_1 + c_2\xi_2 + \cdots + c_r\xi_r + c_{r+j}\xi_{r+j} = 0$$

para $j = 1, 2, \cdots, s - r$. Además, $c_{r+j} \neq 0$. Porque si $c_{r+j} = 0$, el requisito de que no todos los $c_1, c_2, \cdots, c_r, c_{r+j}$ sean cero implicaría, por la ecuación (3), que existen los escalares $c_1, c_2, \cdots, c_r$, no todos cero, tales que $c_1\xi_1 + c_2\xi_2 + \cdots + c_r\xi_r = 0$. Pero esto es imposible puesto que $\xi_1, \xi_2, \cdots, \xi_r$ son linealmente independientes. De aquí que puede despejarse a ξ_{r+j} de la ecuación (3) para obtener ξ_{r+j} como una combinación lineal de $\xi_1, \xi_2, \cdots, \xi_r$ para $j = 1, 2, \cdots, s - r$. De aquí que $\xi_1, \xi_2, \cdots, \xi_r$ generan V cuando $r < s$. Por hipótesis, se cumple la misma conclusión para $r = s$.

Ahora, por el teorema 13, todo conjunto de más de r vectores de V es linealmente dependiente y puesto que, de acuerdo con la definición de dimensión, V contiene m vectores linealmente independiente, se tiene $m \leq r$. Pero como V contiene r vectores linealmente independientes, también se tiene $r \leq m$. De aquí que $r = m$, con lo que se prueba (2) del teorema 14 y, ya que $s \geq r, s \geq m$, lo cual es (1) del teorema 14. Finalmente, (3) se concluye puesto que se ha demostrado que cualquiera de los conjuntos de $r + 1 = m + 1$ vectores $\xi_1, \xi_2, \cdots, \xi_r, \xi_{r+j} (j = 1, 2, \cdots, s - r)$ son linealmente dependientes.

DEFINICIÓN. Un conjunto de vectores $\xi_1, \xi_2, \cdots, \xi_r$ de un espacio vectorial V sobre F se llama *base* de V si (1) los vectores $\xi_1, \xi_2, \cdots, \xi_r$ son linealmente independientes en V y (2) los vectores $\xi_1, \xi_2, \cdots, \xi_r$ generan V.

Teorema 15. Si V es un espacio vectorial de dimensión m sobre F, toda base de V contiene exactamente m vectores (linealmente independientes). Recíprocamente, todo conjunto de m vectores linealmente independientes de V forma una base de V.

Por el teorema 14, una base contiene m, pero no más que m vectores linealmente independientes. Puesto que los vectores de una base son linealmente independientes, una base contiene exactamente m vectores en total.

Recíprocamente, sean $\xi_1, \xi_2, \cdots, \xi_m$ m vectores cualesquiera de V linealmente independientes y sea ξ cualquier otro vector de V. Ya que m es la dimensión de V, los $m + 1$ vectores $\xi_1, \xi_2, \cdots, \xi_m, \xi$ son linealmente dependientes de modo que existen los escalares $c_1, c_2, \cdots, c_m, c$ con $c \neq 0$ tales que

$$c_1\xi_1 + c_2\xi_2 + \cdots + c_m\xi_m + c\xi = 0.$$

De aquí que cualquier vector ξ de V es una combinación lineal de $\xi_1, \xi_2, \cdots, \xi_m$ y, así, $\xi_1, \xi_2, \cdots, \xi_m$ generan V. Puesto que son linealmente independientes, también forman una base de V.

Ejercicios

1. Exhibir tres bases diferentes para $V_3(F)$, donde F es el campo de los números racionales.
2. Encontrar una base para $V_3(F)$, siendo F el campo de los números racionales, el cual incluye los vectores $(1, -1, 1)$ y $(2, 1, 1)$.
3. Demostrar que ninguna base para $V_3(F)$, siendo F el campo de los números racionales, puede incluir tanto al vector $(1, -1, 1)$ como $(2, -2, 2)$.
4. Se dice que dos vectores ξ y η son *ortogonales* si $\xi \cdot \eta = 0$, y se dice que un vector ξ es de *longitud unitaria* si $\xi \cdot \xi = 1$. Una base de un espacio vectorial que consiste de vectores mutuamente ortogonales se llama *base normal ortogonal.*
   a. Probar que los vectores $(2/3, -1/3, 2/3)$, $(2/3, 2/3, -1/3)$ y $(1/3, -2/3, -2/3)$ forman una base ortogonal normal de $V_3(F)$, siendo F el campo de los números racionales.
   b. Encontrar una base normal ortogonal de $V_3(F)$, siendo F el campo de los números reales, de la cual $(1/\sqrt{3}, 1/\sqrt{3}, -1/\sqrt{3})$ es un vector.
   c. Demostrar que los vectores $\xi = (1, 1, -1)$ y $\eta = (2, -1, 1)$ son ortogonales y encontrar un tercer vector que sea ortogonal tanto a ξ como a η.

8 Determinantes y matrices

1 · DEFINICION

Tal y como asociamos un número real $\sqrt{a^2 + b^2}$ a cada número complejo $a + bi$, puede asociarse a cada matriz cuadrada, sobre un campo F, un elemento del campo, conocido como el determinante de la matriz. Sea $A = [a_{ij}]$ una matriz de $n \times n$. Entonces, el determinante de A se denota por $|A| = |a_{ij}|$ y se define como sigue.

Determinante

El determinante $|A|$ de la matriz de $n \times n$, $A = [a_{ij}]$ sobre el campo F, es el polinomio en los elementos a_{ij} de la matriz A que se obtiene de la manera siguiente. Se toma el producto $a_{11}a_{22}\cdots a_{nn}$ de los elementos de la diagonal principal de A y se opera sobre los índices de línea mediante las $n!$ permutaciones $p = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$, donde $i_1, i_2, \cdots, i_n$ son $1, 2, \cdots, n$ en algún orden, obteniendo así $n!$ términos distintos. Si p es una permutación par, se afecta el término con un signo positivo; si p es una permutación impar, se afecta el término con un signo menos. La suma de estos $n!$ términos con signo es el determinante $|A|$.

Denotemos por sgn p, léase signo de p, el signo más si la permutación p es una permutación par y el signo si p es una permutación impar. De este modo, el término obtenido de $a_{11}a_{22}\cdots a_{nn}$, operando sobre los subíndices de línea de estos elementos mediante la permutación p, puede escribirse sgn $p\, a_{i_1 1}a_{i_2 2}\cdots a_{i_n n}$.

EJEMPLO. Encontrar el determinante de $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$. Las permutaciones sobre los símbolos 1 y 2 son la identidad $i = (1)(2)$ y $p = (12)$. Operando

sobre los subíndices de línea de los elementos en $a_{11}a_{22}$, mediante la identidad, se obtiene $a_{11}a_{22}$, y, puesto que la identidad es una permutación par, este término se afecta con un signo más. Operando sobre los subíndices de línea de los elementos en $a_{21}a_{12}$ por la permutación p, se obtiene $a_{12}a_{21}$ y, puesto que p es una permutación impar, este término se afecta con un signo menos. Así

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12}.$$

Orden

El orden de un determinante de una matriz de $n \times n$ es el entero n.

Ejercicios

1. Escribir el determinante de la matriz de 3×3, $A = [a_{ij}]$.
2. Escribir el determinante de la matriz de 4×4, $A = [a_{ij}]$.
3. Encontrar los signos de los siguientes términos en el determinante de la matriz de 5×5, $A = [a_{ij}]$.
   a. [illegible]
   b. [illegible]
   c. [illegible]
4. Probar que el producto de los elementos de la diagonal principal de una matriz es un término en su determinante.
5. Probar que la mitad de los términos en el determinante de una matriz se afectan con un signo más y la otra mitad con un signo menos.

2 · COFACTORES

Nótese que cada término en el determinante $|A|$ contiene un y solamente un elemento de cada línea y cada columna de la matriz A. Por lo tanto, un término que contenga a a_{11}, no contiene otros elementos de la primera línea o la primera columna de A. Agrúpense todos los términos de $|A|$ que contengan al elemento a_{11} como factor. Entonces, la suma de estos términos puede escribirse como $a_{11}C_{11}$. El factor C_{11} se llama *cofactor* de a_{11}. Nótese que los términos en C_{11} se componen de los elementos tomados de la submatriz de A de $(n-1) \times (n-1)$, que se obtiene al suprimir la primera línea y la primera columna de A. En forma semejante, la suma de todos los términos de $|A|$ que contienen al factor a_{ij} puede escribirse como $a_{ij}C_{ij}$, donde, como antes, el factor C_{ij} se llama cofactor de a_{ij}. Los términos de C_{ij} se componen de los elementos de la submatriz M_{ij} de A, que se obtiene al suprimir la i-ésima línea y la j-ésima columna de A. Así, el determinante $|A|$ puede escribirse como una función lineal homogénea de los elementos de la i-ésima línea, simplemente agrupando todos los términos que contengan $a_{i1}, a_{i2}, \cdots, a_{in}$, respectivamente, y formando su suma. Así,

$$|A| = a_{i1}C_{i1} + a_{i2}C_{i2} + \cdots + a_{in}C_{in} = \sum_{j=1}^{n} a_{ij}C_{ij}.$$

En forma semejante, puede escribirse el determinante $|A|$ como una función lineal homogénea de la k-ésima columna agrupando todos los términos que contengan $a_{1k}, a_{2k}, \cdots, a_{nk}$, respectivamente, y formando su suma. Así,

$$|A| = a_{1k}C_{1k} + a_{2k}C_{2k} + \cdots + a_{nk}C_{nk} = \sum_{i=1}^{n} a_{ik}C_{ik}.$$

Estas dos formas de escribir el determinante $|A|$ reciben el nombre de desarrollos de $|A|$ por los elementos y los cofactores de la i-ésima línea y la k-ésima columna de $|A|$. Así, se ha probado el siguiente teorema

Teorema 1. $|A| = \sum_{j=1}^{n} a_{ij}C_{ij}$ *y* $|A| = \sum_{i=1}^{n} a_{ik}C_{ik}$.

El desarrollo de un determinante como una función lineal de sus cofactores nos permite probar la siguiente propiedad de los determinantes.

Teorema 2. Si los elementos de la i*-ésima línea o la* k*-ésima columna de una matriz* A *se multiplican por un elemento* c *del campo, el determinante de la matriz* B *resultante es igual a* c $|A|$.

Ahora, aplicando la primera fórmula del teorema 1, se obtiene $|B| = \sum_{j=1}^{n} ca_{ij}C_{ij} = c\sum_{j=1}^{n} a_{ij}C_{ij} = c|A|$. Para probar el teorema para la k-ésima columna se aplica la segunda fórmula. (Obsérvese que puede tomarse $c = 0$).

Ejercicios

1. En el determinante de la matriz de 3×3, $A = [a_{ij}]$, exhibir los cofactores c_{11}, c_{12}, c_{13}.
2. En el determinante $\begin{vmatrix} 5 & -2 & 1 \\ 3 & 0 & 2 \\ 4 & 1 & 5 \end{vmatrix}$ exhibir los cofactores c_{21}, c_{22}, c_{23}.
3. Demostrar que $\begin{vmatrix} 2 & 3 & 4 \\ 5 & 15 & 5 \\ 2 & 9 & 0 \end{vmatrix} = 15 \begin{vmatrix} 2 & 1 & 4 \\ 1 & 1 & 1 \\ 2 & 3 & 0 \end{vmatrix}$.

3 · PROPIEDADES ADICIONALES

Teorema 3. $|A^t| = |A|$ *donde* A^t *es la transpuesta de la matriz* A.

Sea $A = [a_{ij}]$ una matriz de $n \times n$. Entonces $A^t = [a'_{ij}]$ donde $a'_{ij} = a_{ji}$. Aplicando la definición de un determinante a la matriz A^t. El término general de $|A^t|$ puede escribirse como $s = \operatorname{sgn} p\, a'_{i_1 1} a'_{i_2 2} \cdots a'_{i_n n}$ donde

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix},$$

y $i_1, i_2, \cdots, i_n$ son $1, 2, \cdots, n$ en algún orden. Sustituyendo a_{ji} por a'_{ij} en s, se tiene $s = \operatorname{sgn} p\, a_{1 i_1}, a_{2 i_2}, \cdots a_{n i_n}$. Excepto, tal vez, por el signo, es obvio que éste es un término en $|A|$ puesto que $i_1, i_2, \cdots, i_n$ es una permutación de $1, 2, \cdots, n$. Se determina la permutación p' sobre los subíndices de línea de $d = a_{11} a_{22} \cdots a_{nn}$ que produciría este término. Por lo tanto, el elemento $a_{k i_k}$ en s se obtiene a partir del elemento $a_{i_k k}$ en d, sustituyendo la primera i_k por k. De aquí que

$$p' = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix} = p^{-1}.$$

Ahora, $\operatorname{sgn} p = \operatorname{sgn} p^{-1}$ porque p^{-1} es una permutación par o impar de acuerdo con que p sea una permutación par o impar. Por lo tanto, cada uno de los $n!$ términos de $|A^t|$ es un término de $|A|$ y, de aquí, $|A^t| = |A|$.

El teorema 3 nos permite sustituir cualquier teorema referente a las líneas de un determinante por un teorema semejante referente a sus columnas o viceversa.

Teorema 4. Si en la matriz A *se intercambian dos líneas o dos columnas, el determinante* $|B|$ *de la matriz resultante* B *es igual a* $-|A|$.

Es conveniente probar el teorema para el intercambio de dos columnas. Entonces, el teorema 3 prueba el teorema para el intercambio de dos líneas. Intercámbiense la r-ésima y la s-ésima columnas de A, donde $r < s$, obteniendo la matriz B. El producto de los elementos de la diagonal principal de B es $a_{11} a_{22} \cdots a_{rs} \cdots a_{sr} \cdots a_{nn}$. Entonces, el término general de $|B|$ es $\operatorname{sgn} p\, a_{i_1 1} a_{i_2 2} \cdots a_{i_s s} \cdots a_{i_r r} \cdots a_{i_n n}$, donde

$$p = \begin{pmatrix} 1 & 2 & \cdots & r & \cdots & s & \cdots & n \\ i_1 & i_2 & \cdots & i_s & \cdots & i_r & \cdots & i_n \end{pmatrix}$$

y donde $i_1, i_2, \cdots, i_n$ son $1, 2, \cdots, n$ en algún orden. Una vez más, éste es un término de $|A|$, excepto, tal vez, por el signo. Para obtener este término mediante una permutación de los subíndices de línea de los elementos en la diagonal principal de A, se aplica la permutación

$$q = \begin{pmatrix} 1 & 2 & \cdots & r & \cdots & s & \cdots & n \\ i_1 & i_2 & \cdots & i_s & \cdots & i_r & \cdots & i_n \end{pmatrix}$$

Ahora, $q = pt$, donde $t = (i_r i_s)$. Puesto que t es una transposición, $\operatorname{sgn} q = -\operatorname{sgn} p$. Además, si p recorre las $n!$ permutaciones del grupo simétrico en n símbolos, las permutaciones pt son estas mismas permutaciones en algún orden, ya que, tal y como se vio con anterioridad, si S es un grupo y t es un elemento del grupo, $St = S$.

Corolario. Si una matriz A *tiene dos columnas idénticas o dos líneas idénticas, entonces* $|A| = 0$.

Intercámbiense las dos columnas idénticas de A, obteniendo la matriz B. Entonces, de acuerdo con el teorema anterior, $|B| = -|A|$, pero $B = A$ y de aquí que $|A| = -|A|$ o $|A| + |A| = 0$. Si los elementos de A están en un campo donde $1 + 1 \neq 0$, entonces $|A| = 0$. El corolario también se cumple para los campos en los cuales $1 + 1 = 0$. Ver el ejercicio 3, pág. 168 a fin de obtener una sugerencia para la demostración.

Teorema 5. Sea C_{ij} *el cofactor del elemento* a_{ij} *en el determinante* $|A| = |a_{ij}|$ *de orden* n *y sea* M_{ij} *la submatriz de* A *de* $(n-1) \times (n-1)$ *obtenida suprimiendo la* i*-ésima línea y la* j*-ésima columna de* A. *Entonces* $C_{ij} = (-1)^{i+j}|M_{ij}|$.

Primero se probará que $C_{11} = |M_{11}|$. Recuérdese que la suma de los términos de $|A|$, que contienen a a_{11} como factor, puede escribirse como $a_{11}C_{11}$ y que la totalidad de los elementos de los términos de C_{11} son elementos de la matriz M_{11}. Así, el término general de $a_{11}C_{11}$ es $\operatorname{sgn} p\, a_{11} a_{i_2 2} a_{i_3 3} \cdots a_{i_n n}$, donde

$$p = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}$$

y $i_2, i_3, \cdots, i_n$ son $2, 3, \cdots, n$, en algún orden. Por lo tanto, la permutación p puede considerarse como una permutación sobre los símbolos

$2, 3, \cdots, n$ únicamente. De aquí que todos los términos de $a_{11}C_{11}$ se obtienen haciendo que p recorra las $(n-1)!$ permutaciones sobre los símbolos $2, 3, \cdots, n$, manteniendo fijo a 1. Así, los términos de C_{11} se obtienen operando sobre los subíndices de línea de los elementos del producto $a_{22}a_{33}\cdots a_{nn}$, de los elementos de la diagonal principal de M_{11}. Por lo tanto, $C_{11} = |M_{11}|$.

A continuación se probará que $C_{ij} = (-1)^{i+j}|M_{ij}|$. Se mueve la i-ésima línea de A hacia la primera línea efectuando $i-1$ intercambios sucesivos de las líneas adyacentes de A, y se desplaza la j-ésima columna de A hacia la primera columna, efectuando $j-1$ intercambios sucesivos de columnas adyacentes de A. Llamemos B a la matriz resultante. Así, el elemento a_{ij} está en la primera línea y la primera columna de B y la submatriz de B que se obtiene al suprimir su primera línea y su primera columna, es la submatriz M_{ij} de A. Por lo tanto, los términos de $|B|$ que contienen a a_{ij} son, de acuerdo con la primera parte de esta demostración, $a_{ij}|M_{ij}|$. Pero $|B| = (-1)^{i-1+j-1}|A| = (-1)^{i+j}|A|$ y, de este modo, $|A| = (-1)^{i+j}|B|$. Ahora, los términos de $|A|$ que contienen a a_{ij} como factor son $a_{ij}C_{ij}$ y los términos de $|B|$ que contienen a a_{ij} como factor son $a_{ij}|M_{ij}|$. Por lo tanto, $C_{ij} = (-1)^{i+j}|M_{ij}|$.

El determinante $|M_{ij}|$ se llama *menor* del elemento a_{ij} en el determinante $|A|$. Nótese que ahora el teorema 1 muestra cómo puede desarrollarse un determinante de orden n como una función lineal de determinantes de orden $n-1$.

Teorema 6. Las fórmulas cero. Considérese que C_{ij} *denota el cofactor del elemento* a_{ij} *en el determinante* $|A| = |a_{ij}|$ *de orden* n. *Entonces* $\sum_{j=1}^{n} a_{ij}C_{kj} = 0$ *y* $\sum_{j=1}^{n} a_{ji}C_{jk} = 0$, *si* $i \neq k$.

La primera fórmula es evidente si se recuerda que los cofactores C_{kj}, con $j = 1, 2, \cdots, n$, son determinantes de orden $n-1$ formados a partir de los elementos de $|A|$ que se encuentran en todas las líneas de A, excepto la k-ésima línea. Por lo tanto, si en la suma $\sum_{j=1}^{n} a_{kj}C_{kj}$ se sustituyen los elementos a_{kj} de la k-ésima línea de A por los elementos a_{ij} de la i-ésima línea de A, cuando $i \neq k$, se obtiene la suma deseada. Sin embargo, ahora se ve que esta suma es el determinante de la matriz B, obtenida de A, al sustituir la k-ésima línea de A por su i-ésima línea. Por lo tanto, la matriz B tiene dos líneas iguales y de aquí que $|B| = 0$. En forma semejante, la suma $\sum_{j=1}^{n} a_{ji}C_{jk}$, cuando $i \neq k$, representa el determinante de la matriz C, obtenida de A, al sustituir la k-ésima columna de A por su i-ésima columna. Puesto que C tiene dos columnas iguales, $|C| = 0$.

Teorema 7. Si en la matriz $A = [a_{ij}]$ *de* $n \times n$ *se reemplaza la* k-*ésima línea*, A_k, *de* A, *por la línea* $A_k + cA_i$, *con* $i \neq k$, *el determinante de la matriz resultante es igual al determinante de* A.

Sea B la matriz obtenida de A al sustituir la k-ésima línea de A por $A_k + cA_i$, con $i \neq k$. Desarróllese el determinante B por los elementos y los cofactores de su k-ésima línea. Así,

$$|B| = \sum_{j=1}^{n}(a_{kj} + ca_{ij})C_{kj} = \sum_{j=1}^{n} a_{kj}C_{kj} + c\sum_{j=1}^{n} a_{ij}C_{kj}$$
$$= |A| + 0 = |A|$$

de acuerdo con los teoremas 1 y 6. Es obvio que también se cumple un teorema semejante para las columnas de un determinante.

Los teoremas anteriores se aplican para simplificar la labor de cálculo del valor de un determinante. Si, por ejemplo, en un determinante de orden n todos los elementos, excepto uno, en una línea o columna son cero, el determinante puede escribirse como el producto de este elemento diferente de cero multiplicado por su cofactor, un determinante de orden $n-1$. Aplicando sucesivamente esta regla al determinante de una matriz *diagonal*, es decir, una matriz en la cual todos los términos son cero excepto aquellos que se encuentran en la diagonal principal, se ve que el determinante de una matriz diagonal es el producto de los elementos de la diagonal principal.

EJEMPLO. Apliquemos los teoremas anteriores para evaluar el determinante de Vandermonde de orden 3.

$$|A| = \begin{vmatrix} 1 & 1 & 1 \\ x & y & z \\ x^2 & y^2 & z^2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ x & y-x & z-x \\ x^2 & y^2-x^2 & z^2-x^2 \end{vmatrix}$$
$$= (y-x)(z-x)\begin{vmatrix} 1 & 0 & 0 \\ x & 1 & 1 \\ x^2 & y+x & z+x \end{vmatrix}$$
$$= (y-x)(z-x)\begin{vmatrix} 1 & 1 \\ y+x & z+x \end{vmatrix}$$
$$= (y-x)(z-x)(z-y).$$

Sin embargo, puede evaluarse este determinante en una forma más sencilla observando que, si se desarrolla en términos de los elementos y cofactores de la primera columna, puede considerársele como un polinomio en x. Así, si $x = y$, se ve que el determinante es cero, porque tiene dos columnas iguales. De aquí que $x - y$ es un factor del determinante. En forma semejante, $x - z$ es un factor,

y considerando al determinante como un polinomio en y se ve que $y - z$ es un factor. Así, $|A| = (x - y)(x - z)(y - z)b$, donde b debe determinarse. Puesto que el producto de los elementos de la diagonal principal es un término en $|A|$, yz^2 es un término en $|A|$. El coeficiente de yz^2 en este desarrollo es $-b$. De aquí que $b = -1$. De manera semejante puede probarse que el determinante de Vandermonde de orden n, tiene la siguiente factorización

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i>j}^{n} (x_i - x_j).$$

Ejercicios

1. Encontrar los valores de $\begin{vmatrix} 3 & 4 & -2 & 1 \\ 2 & 4 & 6 & 8 \\ 1 & 8 & 3 & 2 \\ 0 & 0 & 2 & 0 \end{vmatrix}$ y $\begin{vmatrix} 5 & 2 & -1 & 3 \\ 1 & 2 & 1 & 1 \\ -1 & 3 & 0 & 0 \\ 3 & 0 & 0 & 1 \end{vmatrix}$.
2. Sea $|A| = |a_{ij}|$ de orden 4 y sea c_{ij} el cofactor del elemento a_{ij}. Exhibir una matriz cuyo determinante sea igual a $\sum_{j=1}^{4} x_j C_{1j}$. Exhibir una matriz cuyo determinante sea igual a $\sum_{j=1}^{4} x_j C_{j3}$.
3. Probar por inducción que el determinante de una matriz con dos líneas iguales es cero. *Sugerencia:* Comprobar que esto es cierto para un determinante de orden 2. Aplicar el desarrollo por cofactores de un determinante.
4. Sin desarrollar, probar que el determinante *antisimétrico* de orden n impar sobre un campo cuya característica no es 2, es igual a cero; es decir, $|a_{ij}| = 0$, si $a_{ii} = 0$ y $a_{ij} = -a_{ji}$.
5. Probar que $\begin{vmatrix} a_1 + b_1 & c_1 & d_1 \\ a_2 + b_2 & c_2 & d_2 \\ a_3 + b_3 & c_3 & d_3 \end{vmatrix} = \begin{vmatrix} a_1 & c_1 & d_1 \\ a_2 & c_2 & d_2 \\ a_3 & c_3 & d_3 \end{vmatrix} + \begin{vmatrix} b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \\ b_3 & c_3 & d_3 \end{vmatrix}$.
6. Escribir los siguientes determinantes como productos de factores:

a. $\begin{vmatrix} 1 & x & 1 & y \\ x & 1 & y & 1 \\ 1 & y & 1 & x \\ y & 1 & x & 1 \end{vmatrix}$; b. $\begin{vmatrix} b+c & a & a \\ b & c+a & b \\ c & c & a+b \end{vmatrix}$;

c. $\begin{vmatrix} x & a & b & c & 1 \\ d & x & e & f & 1 \\ d & g & x & h & 1 \\ d & g & k & x & 1 \\ d & g & k & m & 1 \end{vmatrix}$; d. $\begin{vmatrix} a & x & y & a \\ x & 0 & 0 & y \\ y & 0 & 0 & x \\ a & y & x & a \end{vmatrix}$;

e. $\begin{vmatrix} a & b & b & b \\ a & b & a & a \\ a & a & b & a \\ b & b & b & a \end{vmatrix}$

7. Sea $A = [a_{ij}]$ una matriz de $n \times n$, con $a_{ij} = 1$ cuando $i \neq j$ y $a_{ii} = 0$. Probar que $|A| = (n - 1)(-1)^{n-1}$.

4 · DESARROLLO DE LAPLACE DE UN DETERMINANTE

DEFINICIÓN. Sea D una submatriz de $r \times r$ de una matriz A de $n \times n$. El determinante de la submatriz D' de A que se obtiene al suprimir las r líneas y las r columnas de A en las cuales se encuentran los elementos de D, se llama *menor complementario* del menor $|D|$.

Teorema 8. El determinante de la matriz $A = [a_{ij}]$ *de* $n \times n$ *es igual a la suma de los productos con signo* $\pm|D_i| \cdot |D_i'|$, *donde* $|D_i|$ *es un menor de* A *de* $r \times r$ *formado a partir de los elementos de las primeras* r *columnas de* A *y donde* $|D_i'|$ *es su menor complementario. Se toma el signo más o el signo menos de acuerdo con que sea necesario un número par o un número impar de intercambios de líneas adyacentes de* A *para llevar la submatriz* D_i *hasta las primeras* r *líneas de* A.

Este procedimiento se llama desarrollo de Laplace por los menores de las primeras r columnas. La prueba hará obvio que pueden tomarse cualesquiera r columnas o r líneas de A si se toman adecuadamente los signos de los productos.

EJEMPLO. $|A| = \begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ d_1 & d_2 & d_3 & d_4 \end{vmatrix}$. Desarrollar por los menores de

las primeras dos columnas. Así

$$|A| = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \cdot \begin{vmatrix} c_3 & c_4 \\ d_3 & d_4 \end{vmatrix} - \begin{vmatrix} a_1 & a_2 \\ c_1 & c_2 \end{vmatrix} \cdot \begin{vmatrix} b_3 & b_4 \\ d_3 & d_4 \end{vmatrix}$$
$$+ \begin{vmatrix} a_1 & a_2 \\ d_1 & d_2 \end{vmatrix} \cdot \begin{vmatrix} b_3 & b_4 \\ c_3 & c_4 \end{vmatrix} + \begin{vmatrix} b_1 & b_2 \\ c_1 & c_2 \end{vmatrix} \cdot \begin{vmatrix} a_3 & a_4 \\ d_3 & d_4 \end{vmatrix}$$
$$- \begin{vmatrix} b_1 & b_2 \\ d_1 & d_2 \end{vmatrix} \cdot \begin{vmatrix} a_3 & a_4 \\ c_3 & c_4 \end{vmatrix} + \begin{vmatrix} c_1 & c_2 \\ d_1 & d_2 \end{vmatrix} \cdot \begin{vmatrix} a_3 & a_4 \\ b_3 & b_4 \end{vmatrix}$$

DEMOSTRACIÓN. Sea

$$|D_1| = \begin{vmatrix} a_{11} & \cdots & a_{1r} \\ \cdot & \cdots & \cdot \\ a_{r1} & \cdots & a_{rr} \end{vmatrix} \quad \text{y} \quad |D_1'| = \begin{vmatrix} a_{r+1,r+1} & \cdots & a_{r+1,n} \\ \cdot & \cdots & \cdot \\ a_{n,r+1} & \cdots & a_{nn} \end{vmatrix}.$$

Aplíquese la definición de determinante a $|D_1|$ y a $|D_1'|$. El término general en $|D_1|$ es sgn $p\, a_{i_1 1} a_{i_2 2} \cdots a_{i_r r}$, donde

$$p = \begin{pmatrix} 1 & 2 & \cdots & r \\ i_1 & i_2 & \cdots & i_r \end{pmatrix}$$

y donde $i_1, i_2, \cdots, i_r$ son $1, 2, \cdots, r$, en algún orden. El término general en D_1' es sgn $q\, a_{i_{r+1} r+1} \cdots a_{i_n n}$, donde

$$q = \begin{pmatrix} r+1 & \cdots & n \\ i_{r+1} & \cdots & i_n \end{pmatrix}$$

y donde $i_{r+1}, \cdots, i_n$ son $r+1, \cdots, n$, en algún orden. Es evidente que el término general en el producto $|D_1| \cdot |D_1'|$ es (sgn p) (sgn q) $a_{i_1 1} \cdots a_{i_r r} a_{i_{r+1} r+1} \cdots a_{i_n n}$. Este es un término en $|A|$ puesto que puede obtenerse de la diagonal principal de A mediante la permutación pq. Por lo tanto, todo término en $|D_1| \cdot |D_1'|$ es un término de $|A|$. Ahora considérese el producto $|D_i| \cdot ||D_i'|$, con $i > 1$. Intercámbiense las líneas adyacentes de A de manera que la submatriz D_i se encuentre en las primeras r líneas de la matriz resultante B. Como en el primer caso discutido, los términos de $|D_i| \cdot |D_i'|$ son términos de $|B|$. Si B se ha obtenido de A haciendo k intercambios de líneas adyacentes, entonces $|B| = (-1)^k|A|$ y de aquí que los términos de $(-1)^k|D_i| \cdot |D_i'|$ son términos de $|A|$. Es evidente que los términos de $|D_i| \cdot |D_i'|$ y $|D_j| \cdot |D_j'|$, con $j \neq i$, son distintos. Existen $C(n, r) = n!/[r!(n - r!)]$ productos $|D_i| \cdot |D_i'|$ y cada producto contiene $r!(n - r)!$ términos. Por lo tanto, la suma de estos productos con signo contiene $C(n, r)r!(n - r)! = n!$ términos. Así, se ha verificado el desarrollo de Laplace.

Ejercicios

1. Desarrollar, aplicando el procedimiento de Laplace, por los menores de las dos primeras columnas y simplificar la suma resultante:

$$\begin{vmatrix} a & 1 & 0 & 0 & 0 \\ b & a & 1 & 0 & 0 \\ 0 & b & a & 1 & 0 \\ 0 & 0 & b & a & 1 \\ 0 & 0 & 0 & b & a \end{vmatrix}$$

2. Expresar como el producto de dos determinantes de orden 2:

$$\begin{vmatrix} 0 & 1 & x & y \\ 1 & 0 & y & x \\ z & w & 0 & 0 \\ w & z & 0 & 0 \end{vmatrix}.$$

3. Probar que:

$$\begin{vmatrix} a & b & c & d \\ e & f & g & h \\ 0 & 0 & j & k \\ 0 & 0 & l & m \end{vmatrix} = \begin{vmatrix} a & b \\ e & f \end{vmatrix} \cdot \begin{vmatrix} j & k \\ l & m \end{vmatrix}.$$

4. Aplicando menores de dos líneas de las primeras dos líneas, demostrar que

$$\frac{1}{2}\begin{vmatrix} a & b & c & d \\ e & f & g & h \\ a & b & c & d \\ e & f & g & h \end{vmatrix} = \begin{vmatrix} a & b \\ e & f \end{vmatrix} \cdot \begin{vmatrix} c & d \\ g & h \end{vmatrix} - \begin{vmatrix} a & c \\ e & g \end{vmatrix} \cdot \begin{vmatrix} b & d \\ f & h \end{vmatrix} + \begin{vmatrix} a & d \\ e & h \end{vmatrix} \cdot \begin{vmatrix} b & c \\ f & g \end{vmatrix} = 0.$$

5 · PRODUCTOS DE DETERMINANTES

A continuación, se desarrollarán algunas propiedades del producto de determinantes. El determinante de la matriz identidad I de $n \times n$ es 1. Sea E una matriz obtenida de la matriz identidad efectuando una operación elemental sobre las líneas. Es obvio, con base en las propiedades

de los determinantes, que $|E| = -1, c$ o 1, de acuerdo con que se haya efectuado en I la primera, la segunda o la tercera operación elemental sobre las líneas. Ahora, sea A una matriz de $n \times n$. Entonces $|EA| = -|A|$, $c|A|$ o $|A|$ y $|EA| = |AE|$. De aquí que se ha probado el teorema siguiente.

Teorema 9. Si E *es una matriz elemental,* $|\mathrm{EA}| = |\mathrm{AE}| = |\mathrm{E}| \cdot |\mathrm{A}| = |\mathrm{A}| \cdot |\mathrm{E}|$.

Se aplicará este teorema para probar el teorema siguiente.

Teorema 10. Una matriz A *de* $n \times n$ *es no singular si y solamente si* $|\mathrm{A}| \neq 0$.

Sea C la forma canónica de la matriz A. Entonces existen las matrices no singulares S y T tales que $SAT = C$. De aquí que $A = S^{-1}CT^{-1} = E_1E_2 \cdots E_sC\,E_1'E_2' \cdots E_t'$, donde los E_i y los E_i' son matrices elementales. Ahora, haciendo aplicaciones sucesivas del teorema 9, se tiene $|A| = |E_1E_2 \cdots E_sCE_1'E_2' \cdots E_t'| = |E_1| \cdot |E_2| \cdots |E_s| \cdot |C| \cdot |E_1'| \cdot |E_2'| \cdots |E_t'|$. Y puesto que los determinantes de las matrices elementales no son cero, se ve que $|A| = 0$ si y solamente si $|C| = 0$. Pero $|C| = 0$ si y solamente si tiene una línea de ceros, es decir, si y solamente si A es de rango $< n$. Así, A es no singular si y solamente si $|A| \neq 0$.

El teorema siguiente nos da una regla para multiplicar dos determinantes de orden n para obtener un determinante de orden n. Simplemente se multiplican las matrices de los dos determinantes y se encuentra el determinante de la matriz resultante.

Teorema 11. $|\mathrm{AB}| = |\mathrm{A}| \cdot |\mathrm{B}|$.

Sean C_a y C_b las formas canónicas de las matrices A y B, respectivamente. Entonces $A = D_1D_2 \cdots D_rC_aE_1E_2 \cdots E_s$ y $B = F_1F_2 \cdots F_tC_bG_1G_2 \cdots G_u$, donde los D_i, E_i, F_i y G_i son matrices elementales. Por lo tanto,

$$AB = D_1D_2 \cdots D_rC_aE_1E_2 \cdots E_sF_1F_2 \cdots F_tC_bG_1G_2 \cdots G_u,$$

y, aplicando el teorema 9, se tiene

$$|AB| = |D_1D_2 \cdots D_r| \cdot |C_aE_1E_2 \cdots E_sF_1F_2 \cdots F_tC_b| \cdot |G_1G_2 \cdots G_u|$$

Ahora, si A y B son no singulares, C_a y C_b son matrices identidad y, aplicando otra vez el teorema 9, se tiene

$$\begin{aligned}|AB| &= |D_1D_2 \cdots D_rC_aE_1E_2 \cdots E_s| \cdot |F_1F_2 \cdots F_tC_bG_1G_2 \cdots G_u| \\ &= |A| \cdot |B|.\end{aligned}$$

Si A es singular, C_a tiene una línea de ceros y de aquí que $M = C_aE_1E_2$ $\cdots E_sF_1F_2 \cdots F_tC_b$ tiene una línea de ceros. Por lo tanto, $|M| = 0$ y $|AB| = 0$. Si B es singular, C_b tiene una columna de ceros y de aquí que M tiene una columna de ceros, dando otra vez $|M| = 0$ y $|A| = 0$. Ahora, si A o B es singular, $|A| \cdot |B| = 0$ y de aquí que $|AB| = |A| \cdot |B|$.

Teorema 12. $|\mathrm{AB}^t| = |\mathrm{A}| \cdot |\mathrm{B}|$, *donde* B^t *es la transpuesta de la matriz* B.

Obsérvese que este teorema indica un segundo camino para multiplicar dos determinantes de orden n: simplemente se encuentra el determinante de la matriz AB^t. Para establecer el resultado vagamente, este teorema nos proporciona una regla de línea por línea para la multiplicación de dos determinantes. La demostración consiste en observar que $|AB^t| = |A| \cdot |B^t| = |A| \cdot |B|$, porque el determinante de la transpuesta de una matriz es igual al determinante de la matriz.

EJEMPLO. $\begin{vmatrix} 1 & 2 \\ -1 & 3 \end{vmatrix} \cdot \begin{vmatrix} 0 & -1 \\ 2 & 1 \end{vmatrix} = \begin{vmatrix} 4 & 1 \\ 6 & 4 \end{vmatrix}$ si la multiplicación se ha efectuado aplicando la regla de línea por columna, pero el producto $= \begin{vmatrix} -2 & 4 \\ -3 & 1 \end{vmatrix}$ si se ha efectuado la multiplicación aplicando la regla de línea por línea.

Ejercicios

1. Si $s_i = a^i + b^i + c^i$ para $i = 1, 2, 3$ y 4, probar que:

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} \cdot \begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix} = \begin{vmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix}.$$

2. Probar que:

$$\begin{vmatrix} aa' + bb' + cc' & ea' + fb' + gc' \\ ae' + bf' + cg' & ee' + ff' + gg' \end{vmatrix} =$$

$$\begin{vmatrix} a & b \\ e & f \end{vmatrix} \cdot \begin{vmatrix} a' & b' \\ e' & f' \end{vmatrix} + \begin{vmatrix} a & c \\ e & g \end{vmatrix} \cdot \begin{vmatrix} a' & c' \\ e' & g' \end{vmatrix} + \begin{vmatrix} b & c \\ f & g \end{vmatrix} \cdot \begin{vmatrix} b' & c' \\ f' & g' \end{vmatrix}$$

6 · ADJUNTA E INVERSA DE UNA MATRIZ

DEFINICIÓN. Sea $A = [a_{ij}]$ una matriz de $n \times n$. Sea C_{ij} el cofactor del elemento a_{ij}. Entonces la matriz $[C_{ji}']$, donde el elemento C_{ji}' en la j-ésima línea y la i-ésima columna es igual a C_{ij} se llama la *adjunta* de A, denotada frecuentemente por adj A.

Teorema 13. $A(adj\, A) = |A|I$ *y* $(adj\, A) = |A|I$.

El elemento en la k-ésima línea y la i-ésima columna del producto $A[C_{ji}']$ es $\sum_{j=1}^{n} a_{kj}C_{ji}' = \sum_{j=1}^{n} a_{kj}C_{ij}$, el cual, de acuerdo con el teorema 6, es igual a cero si $k \neq i$ y que, de acuerdo con el teorema 1, es igual a $|A|$ si $k = i$. De aquí que $A(\text{adj}\, A)$ es una matriz diagonal con elementos diagonales iguales a $|A|$. Por lo tanto, $A(\text{adj}\, A) = |A|I$. En forma semejante, el elemento en la j-ésima línea y la k-ésima columna del producto $[C_{ji}']A$ es $\sum_{i=1}^{n} C_{ji}'a_{ik} = \sum_{i=1}^{n} C_{ij}a_{ik}$, el cual es igual a cero si $j \neq k$ e igual a $|A|$ si $j = k$.

De aquí que, de la definición de la inversa de una matriz, se tiene el corolario siguiente.

Corolario. $A^{-1} = (adj\, A)/|A|$.

EJEMPLO. La adjunta de la matriz

$$A = \begin{bmatrix} 2 & -1 & 3 \\ 0 & 2 & 0 \\ 2 & 1 & 1 \end{bmatrix} \text{ es}$$

$$\begin{bmatrix} \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix} & -\begin{vmatrix} -1 & 3 \\ 1 & 1 \end{vmatrix} & \begin{vmatrix} -1 & 3 \\ 2 & 0 \end{vmatrix} \\ -\begin{vmatrix} 0 & 0 \\ 2 & 1 \end{vmatrix} & \begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 2 & 3 \\ 0 & 0 \end{vmatrix} \\ \begin{vmatrix} 0 & 2 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 2 & -1 \\ 2 & 1 \end{vmatrix} & \begin{vmatrix} 2 & -1 \\ 0 & 2 \end{vmatrix} \end{bmatrix} = \begin{bmatrix} 2 & 4 & -6 \\ 0 & -4 & 0 \\ -4 & -4 & 4 \end{bmatrix}$$

$$y \quad A(\text{adj}\, A) = \begin{bmatrix} -8 & 0 & 0 \\ 0 & -8 & 0 \\ 0 & 0 & -8 \end{bmatrix} = -8\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} -1/4 & -1/2 & 3/4 \\ 0 & 1/2 & 0 \\ 1/2 & 1/2 & -1/2 \end{bmatrix}.$$

Ejercicios

1. Efectuar la multiplicación de los dos determinantes en dos formas y presentar los determinantes que resulten:

a. $\begin{vmatrix} 1 & -1 & 2 \\ 3 & 4 & 1 \\ 0 & 2 & 2 \end{vmatrix} \cdot \begin{vmatrix} 0 & 2 & 1 \\ 0 & 1 & 1 \\ 2 & -1 & 1 \end{vmatrix}.$

b. $\begin{vmatrix} a & 0 & a \\ b & 0 & b \\ c & c & c \end{vmatrix} \cdot \begin{vmatrix} 1 & 1 & -1 \\ 2 & 0 & 2 \\ 1 & 1 & 1 \end{vmatrix}.$

2. Encontrar las adjuntas y las inversas de las siguientes matrices:

a. $\begin{bmatrix} 1 & 2 & 3 \\ 0 & 5 & 0 \\ 2 & 4 & 3 \end{bmatrix}$; b. $\begin{bmatrix} 3 & -1 & 2 \\ 1 & 0 & 3 \\ 4 & 0 & 2 \end{bmatrix}$; c. $\begin{bmatrix} 2 & 3 & -1 \\ 0 & 1 & -1 \\ 2 & 1 & 2 \end{bmatrix}$

3. Encontrar el producto $A(\text{adj}\, A)$ si $A = \begin{bmatrix} 3 & 2 & -1 \\ 1 & -3 & 2 \\ 5 & -4 & 3 \end{bmatrix}$

4. Sea A una matriz de $n \times n$. Probar que el determinante de la adjunta de A es $|A|^{n-1}$.
5. Sea A una matriz de $n \times n$. Probar que la adjunta de la adjunta de A es $|A|^{n-2}A$.

7 · REGLA DE CRAMER

El último corolario prueba la regla de Cramer para resolver n ecuaciones lineales simultáneas con n incógnitas.

Teorema 14. Si las n *ecuaciones lineales simultáneas con* n *incógnitas* $\sum_{j=1}^{n} a_{ij}x_j = c_i$, *con* $i = 1, 2, \cdots n$, *tienen un determinante de los coeficientes diferente de cero* $|A| = |a_{ij}|$, *entonces las ecuaciones tienen las soluciones únicas* $x_j = (C_{1j}c_1 + C_{2j}c_2 + \cdots + C_{nj}c_n)/|A|$, *con* $j = 1, 2, \cdots n$, *donde* C_{ij} *es el cofactor del elemento* a_{ij} *en* $|A|$.

Haciendo $X^t = [x_1, x_2, \cdots, x_n]$ y $C^t = [c_1, c_2, \cdots, c_n]$, escríbanse las ecuaciones en forma matricial como $AX = C$. Entonces, la solución es, tal y como se vio con anterioridad, $X = A^{-1}C$. La forma de la solución en el teorema se encuentra aplicando $A^{-1} = (\text{adj}\, A)/|A|$. Por lo tanto, el elemento en la j-ésima línea de la solución matricial es

$$x_j = \sum_{i=1}^{n} \frac{C_{ij}'c_i}{|A|} = \sum_{i=1}^{n} \frac{C_{ij}c_i}{|A|}.$$

Nótese que el numerador en la solución es

$$\begin{vmatrix} a_{11} \cdots a_{1,j-1} & c_1 & a_{1,j+1} \cdots a_{1n} \\ a_{21} \cdots a_{2,j-1} & c_2 & a_{2,j+1} \cdots a_{2n} \\ \cdots\cdots\cdots & \cdots & \cdots\cdots\cdots \\ a_{n1} \cdots a_{n,j-1} & c_n & a_{n,j+1} \cdots a_{nn} \end{vmatrix}$$

que es el determinante obtenido al sustituir la j-ésima columna de $|A|$ por las constantes c_i, $i = 1, 2, \cdots, n$.

Ejercicios

Aplicar la regla de Cramer para encontrar las soluciones de las siguientes ecuaciones:

1. $2x + 3y - 4z = -8$, $3x + 2y + 4z = 3$, $5x - 4y + 5z = 18$.
2. $3x + y + z + w = 0$, $2x - y + 2z - w = 4$, $x + 2z + w = 3$, $2x + 3z + w = 1$.
3. $x + y + z = 11$, $2x - 6y - z = 0$, $3x + 4y + 2z = 0$.
4. $2x - y + 3z - 2w = 4$, $x + 7y + z - w = 2$, $3x + 5y - 5z + 3w = 0$, $4x - 3y + 2z - w = 5$.

8 · RANGO DETERMINANTE DE UNA MATRIZ

DEFINICIÓN. Se dice que una matriz A de $m \times n$ es de *rango determinante d*, si existe una submatriz D de $d \times d$ de A cuyo determinante $|D| \neq 0$ y si el determinante de toda submatriz de A de $(d+1) \times (d+1)$ es cero.

Obsérvese que esta definición implica que el determinante de toda submatriz de A de $r \times r$, con $r > d + 1$, es cero porque un determinante es una función lineal homogénea de los cofactores de una línea o una columna y los cofactores son determinantes de orden $r - 1$ si el determinante es de orden r. Así, cualquier determinante de orden $r > d + 1$ puede, finalmente, expresarse como una suma lineal de determinantes de orden $d + 1$ y de aquí que debe ser cero.

Teorema 15. El rango de una matriz es igual a su rango determinante.

Sea d el rango determinante de una matriz A y r su rango. Por lo tanto, A tiene una submatriz D de $d \times d$ cuyo determinante $|D| \neq 0$. Considérense aquellas líneas de A en las cuales se encuentra D. Las líneas de D son linealmente independientes puesto que D es no singular. De aquí que las d líneas de A que contribuyen con elementos para las líneas de D, son linealmente independientes porque una relación lineal líneas de D, son linealmente independientes porque una relación lineal entre las líneas de A también proporciona una relación lineal entre las líneas correspondientes de D. De aquí que el número máximo r de líneas de A linealmente independientes, por lo menos es d; es decir, $r \geq d$. A continuación, se probará que $r \leq d$. Considérense r líneas de A que sean linealmente independientes y denotemos por R la submatriz de A de $r \times n$ formada por estas r líneas. Ahora, puesto que el rango línea de R es r, su rango columna también es r. De aquí que R tiene r columnas linealmente independientes. Sea R_1 la submatriz de R de $r \times r$ formada por estas columnas linealmente independientes. Es no singular y de aquí que $|R_1| \neq 0$. Pero R_1 también es una submatriz de A. De aquí que $r \leq d$. Recordando la desigualdad anterior $r \geq d$, se concluye que $r = d$.

Nótese que, incidentalmente, se ha probado el útil corolario siguiente.

Corolario. d *líneas cualesquiera de una matriz que contienen una submatriz de* d $\times$ d *cuyo determinante no es cero, son linealmente independientes.*

Ejercicios

Determinar si las líneas de cada una de las matrices siguientes son linealmente dependientes. Si son linealmente dependientes, encontrar un subconjunto máximo que sea linealmente independiente.

a. $\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 2 & 1 & 0 & 2 \\ 4 & -1 & 2 & -4 \end{bmatrix}$;

b. $\begin{bmatrix} 3 & 4 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 2 & 3 & -2 & 2 \\ 5 & 7 & -3 & 3 \end{bmatrix}$;

c. $\begin{bmatrix} 2 & 3 & -4 & 5 \\ 1 & -1 & 2 & -1 \\ 4 & 1 & 0 & 3 \\ 7 & 3 & -2 & 7 \end{bmatrix}$;

d. $\begin{bmatrix} 2 & -1 & 3 & 2 \\ 1 & 7 & 1 & 1 \\ 3 & 5 & -5 & 0 \\ 4 & -3 & 2 & 1 \end{bmatrix}$.

9 · POLINOMIOS CON COEFICIENTES MATRICIALES

Sean $A_0, A_1, \cdots, A_r$ matrices de $n \times n$ sobre un campo F. Se construye el polinomio

$$f(x) = A_0 + A_1x + A_2x^2 + \cdots + A_rx^r$$

en la indeterminada x. El símbolo x es para actuar como un escalar respecto de los coeficientes matriciales. Así, $f(x)$ también puede considerarse como una matriz. Por ejemplo, puede escribirse

$$f(x) = \begin{bmatrix} 1 & 0 \\ 2 & -1 \end{bmatrix} + \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix} x + \begin{bmatrix} 3 & 1 \\ 0 & 1 \end{bmatrix} x^2$$
$$= \begin{bmatrix} 1 + x + 3x^2 & -x + x^2 \\ 2 & -1 + x^2 \end{bmatrix}.$$

Si $g(x) = B_0 + B_1x + \cdots + B_mx^m$, donde $B_0, B_1, \cdots, B_m$ también son matrices de $n \times n$ sobre el campo F, pueden definirse la suma y el producto de $f(x)$ y $g(x)$ en la forma acostumbrada:

$$\begin{aligned} f(x) + g(x) &= (A_0 + B_0) + (A_1 + B_1)x + \cdots \\ &\quad + (A_m + B_m)x^m + A_{m+1}x^{m+1} + \cdots + A_rx^r, \quad r \geq m, \\ h(x) = f(x) \cdot g(x) &= A_0B_0 + (A_0B_1 + A_1B_0)x + \cdots \\ &\quad + (A_0B_k + A_1B_{k-1} + \cdots + A_kB_0)x^k + \cdots + A_rB_mx^{r+m} \end{aligned}$$

Estamos interesados en definir un valor funcional de $f(x)$ cuando se sustituye una matriz C por x. Ya que la multiplicación de matrices no es conmutativa, es obvia la necesidad de la definición, porque ahora se ve que se sustituye x por un símbolo que ya no es conmutativo con cada matriz. Por ejemplo, si

$$f(x) = \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} + \begin{bmatrix} 2 & -1 \\ 3 & 2 \end{bmatrix} x = \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} + x \begin{bmatrix} 2 & -1 \\ 3 & 2 \end{bmatrix},$$

y si se desea sustituir $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ por x, se observa que la matriz

$$\begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} + \begin{bmatrix} 2 & -1 \\ 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix}$$
$$+ \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 2 & -1 \\ 3 & 2 \end{bmatrix}.$$

De aquí que se defina un *valor funcional derecho* $f_D(C)$ y un *valor funcional izquierdo* $f_I(C)$, de la manera siguiente:

$$f_D(C) = A_0 + A_1C + A_2C^2 + \cdots + A_rC^r$$

y

$$f_I(C) = A_0 + CA_1 + C^2A_2 + \cdots + C^rA_r.$$

Fácilmente se ve que, si $f(x) \cdot g(x) = h(x)$, no se sigue necesariamente que $f_D(C) \cdot g_D(C) = h_D(C)$. Sin embargo, puede probarse el teorema siguiente.

Teorema 16. Sea $\mathrm{f(x) \cdot g(x) = h(x)}$, *donde* $\mathrm{f(x), g(x)}$ *y* $\mathrm{h(x)}$ *son polinomios cuyos coeficientes son matrices de* $\mathrm{n \times n}$ *tal que* $\mathrm{g_D(C) = 0}$. *Entonces,* $\mathrm{h_D(C) = 0}$.

Aplicando la notación dada anteriormente para $f(x)$, $g(x)$ y $h(x)$, se tiene

$$\begin{aligned} h_D(C) &= A_0B_0 + (A_0B_1 + A_1B_0)C + (A_0B_2 + A_1B_1 + A_2B_0)C^2 \\ &\quad + \cdots + A_rB_mC^{r+m} \\ &= A_0(B_0 + B_1C + B_2C^2 + \cdots + B_mC^m) \\ &\quad + A_1(B_0 + B_1C + \cdots + B_mC^m)C + \cdots \\ &\quad + A_k(B_0 + B_1C + \cdots + B_mC^m)C^k + \cdots \\ &\quad + A_n(B_0 + B_1C + \cdots + B_mC^m)C^r \\ &= A_0g_D(C) + A_1g_D(C)C + \cdots + A_rg_D(C)C^r. \end{aligned}$$

Así, si $g_D(C) = 0$, $h_D(C) = 0$. En forma semejante puede probarse que, si $f_I(C) = 0$, entonces $h_I(C) = 0$.

Con base en estas observaciones se ve que la teoría de los polinomios con coeficientes matriciales es más complicada que la teoría de los polinomios sobre un campo.

Polinomio característico de una matriz

Sea A una matriz de $n \times n$ sobre un campo F. Se construye la matriz $A - xI$, donde I es la matriz identidad de $n \times n$ y x es un indeterminado. El determinante $|A - xI| = b_0 + b_1x + \cdots + (-1)^nx^n = f(x)$ se llama *polinomio característico* de la matriz A.

EJEMPLO. Sea $A = \begin{bmatrix} 2 & -1 \\ -6 & 1 \end{bmatrix}$, entonces

$$A - xI = \begin{bmatrix} 2 - x & -1 \\ -6 & 1 - x \end{bmatrix}$$

y $A - xI = -4 - 3x + x^2 = f(x)$. Un cálculo sencillo demuestra que $-4I - 3A + A^2$ es la matriz cero.

A continuación se probará que, en general, si se sustituye una matriz A por x en su polinomio característico, y si el término constante en el polinomio se multiplica por la matriz identidad, la suma resultante es la matriz cero. Así, se dice que una matriz A es un cero de un polinomio característico.

Teorema 17. Teorema de Cayley-Hamilton. Sea A *una matriz de* $n \times n$ *sobre un campo y sea* $f(x) = b_0 + b_1x + b_2x^2 + \cdots + (-1)^n x^n$ *su polinomio característico. Entonces* $b_0I + b_1A + b_2A^2 + \cdots + (-1)^n A^n = 0$.

Ahora, $\operatorname{adj}(A - xI) \cdot (A - xI) = f(x)I$. Los elementos de $\operatorname{adj}(A - xI)$ son polinomios en x cuyo grado es cuando más $n - 1$, con coeficientes sobre el campo F. De aquí que $\operatorname{adj}(A - xI)$ puede considerarse como un polinomio en x cuyo grado es cuando más $n - 1$, con coeficientes matriciales sobre F. Así, $\operatorname{adj}(A - xI) \cdot (A - xI)$ es el producto de dos polinomios con coeficientes matriciales, los cuales son iguales a un polinomio en x de grado n cuyos coeficientes son matrices escalares sobre F. Nótese que $A - AI = 0$. De aquí que, de acuerdo con el teorema previo, $f_D(A)I = 0$, pero, puesto que los coeficientes de $f(x)I$ son matrices escalares, los valores funcionales derecho e izquierdo son los mismos. De aquí que puede escribirse $f(A)I = 0$, que es el resultado deseado.

DEFINICIÓN. Los ceros del polinomio característico de una matriz sobre un campo F se llaman *raíces características** de la matriz. Si el campo F es el campo de los números complejos, entonces el polinomio característico de una matriz de $n \times n$ sobre F siempre tiene n ceros que son números complejos.

Las raíces características de la matriz A, en el ejemplo anterior, son -1 y 4.

Ejercicios

Formar el polinomio característico y encontrar las raíces características de las matrices siguientes sobre el campo de los números complejos.

* Llamados también *eigenvalores*.

1. $\begin{bmatrix} 3 & 2 \\ -2 & 3 \end{bmatrix}$.
2. $\begin{bmatrix} 1 & -6 \\ 2 & -6 \end{bmatrix}$.
3. $\begin{bmatrix} 1 & 3 \\ -1 & 5 \end{bmatrix}$.
4. $\begin{bmatrix} i & -2i \\ 0 & -i \end{bmatrix}$.
5. $\begin{bmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$.
6. $\begin{bmatrix} 3 & 2 & 2 \\ 1 & 4 & 1 \\ -2 & -4 & -1 \end{bmatrix}$.
7. Probar el teorema de Cayley-Hamilton para las matrices de 2×2 mediante el cálculo directo.
8. Encontrar una condición necesaria y suficiente para que las raíces características de una matriz de 2×2 sean iguales.
9. Encontrar todas las matrices de 2×2 cuyas raíces características sean 1 y -1.

10 · MATRICES SEMEJANTES SOBRE UN CAMPO

DEFINICIÓN. Si existe una matriz S no singular tal que $S^{-1}AS = B$, entonces se dice que A y B son semejantes.

Nótese que la semejanza de matrices es un caso especial de la equivalencia de matrices. Se darán algunas de las propiedades más sencillas de las matrices semejantes.

Teorema 18. Los determinantes de las matrices semejantes son iguales.

Sea $B = S^{-1}AS$. Entonces $|B| = |S^{-1}AS| = |S^{-1}| \cdot |A| \cdot |S| = |A| \cdot |S^{-1}| \cdot |S| = |A| \cdot |S^{-1}S| = |A| \cdot |I| = |A|$.

Teorema 19. Las matrices semejantes tienen el mismo polinomio característico.

Sea $B = S^{-1}AS$. Entonces

$$B - xI = S^{-1}AS - xI = S^{-1}AS - S^{-1}(xI)S$$
$$= S^{-1}(AS - xIS) = S^{-1}(A - xI)S.$$

De aquí que

$$|B - xI| = |S^{-1}| \cdot |A - xI| \cdot |S| = |A - xI|.$$

Las matrices diagonales tienen propiedades particularmente sencillas. Por ejemplo, sus determinantes son los productos de los elementos que se encuentran en su diagonal principal y el producto de dos matrices diagonales es una matriz diagonal. Además, el polinomio característico de una matriz diagonal cuyos elementos diagonales son $d_1, d_2, \cdots, d_n$ es $(d_1 - x)(d_2 - x)\cdots(d_n - x)$ y de aquí que sus raíces características son $d_1, d_2, \cdots, d_n$. Es interesante examinar un ejemplo sencillo de una matriz que es semejante a una matriz diagonal.

Teorema 20. Sea A *una matriz de* n $\times$ n *sobre el campo de los números complejos. Si las raíces características de la matriz* A *son distintas, entonces* A *es semejante a una matriz diagonal.*

Considérese que $|A - xI| = f(x)$ tiene los ceros distintos $r_1, r_2, \cdots, r_n$. Se construye una matriz S no singular tal que $S^{-1}AS$ sea una matriz diagonal en la que los elementos diagonales son $r_1, r_2, \cdots, r_n$. Primero se demostrará que pueden encontrarse matrices, o vectores, de $n \times 1$, S_j, tales que $AS_j = r_jS_j$ para $j = 1, 2, \cdots, n$. Denotemos los elementos de S_j por $s_{1j}, s_{2j}, \cdots, s_{nj}$. Ahora, $AS_j = r_jS_j$ puede escribirse como $(A - r_jI)S_j = 0$ que, para cada $j = 1, 2, \cdots, n$, es un sistema de n ecuaciones lineales homogéneas con las n incógnitas s_{ij}, con $i = 1, 2, \cdots, n$. Este sistema tiene una solución diferente a $(0, 0, \cdots, 0)$ si y solamente si el determinante $|A - r_jI| = 0$. Pero, r_j es un cero de $f(x)$, y de aquí que se tienen las soluciones diferentes de cero deseadas para cada j. Las columnas de la matriz S son las n columnas S_j.

A continuación se demostrará que los n vectores S_j son linealmente independientes. Supóngase que existe una relación lineal $\sum_{j=1}^{n} c_jS_j = 0$ El método que se aplica para demostrar que $c_1 = 0$, por ejemplo, puede aplicarse para probar que cada $c_j = 0$ para $j = 1, 2, \cdots, n$. Multiplíquese el primer miembro de la ecuación matricial $\sum_{j=1}^{n} c_jS_j = 0$ por el producto

$$(A - r_2I)(A - r_3I)\cdots(A - r_nI),$$

obteniendo

$$(A - r_2I)(A - r_3I)\cdots(A - r_nI)(c_1S_1 + c_2S_2 + \cdots + c_nS_n) = 0.$$

Nótese que los factores $(A - r_jI)$ son conmutativos, uno con respecto a otro. Ahora,

$$\begin{aligned}(A - r_jI)c_kS_k &= (AS_k - r_jS_k)c_k = (r_kS_k - r_jS_k)c_k\\ &= (r_k - r_j)S_kc_k,\end{aligned}$$

de modo que

$$(A - r_jI)c_jS_j = 0.$$

Por lo tanto,

$$\begin{aligned}&(A - r_2I)(A - r_3I)\cdots(A - r_nI)(c_1S_1 + c_2S_2 + \cdots + c_nS_n)\\ &= (A - r_2I)(A - r_3I)\cdots(A - r_nI)c_1S_1\\ &= (r_1 - r_2)(r_1 - r_3)\cdots(r_1 - r_n)c_1S_1 = 0,\end{aligned}$$

si y solamente si $c_1 = 0$. De aquí que las columnas S_j son linealmente independientes de manera que S es no singular. Puesto que $AS_j = r_jS_j$, donde las S_j son las columnas de S, se tiene

$$AS = S\begin{bmatrix} r_1 & 0 & 0 & \cdots & 0 \\ 0 & r_2 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & r_n \end{bmatrix}$$

y finalmente, que $S^{-1}AS$ es una matriz diagonal.

EJEMPLO. Siendo $A = \begin{bmatrix} 2 & -1 \\ -6 & 1 \end{bmatrix}$, se tiene $f(x) = |A - xI| = (x - 4)(x + 1)$ que tiene los dos ceros 4 y -1. Se resuelven los dos sistemas de ecuaciones $AS_1 = 4S_1$ y $AS_2 = -S_2$. Así se tiene $(A - 4I)S_1 = 0$ y $(A + I)S_2 = 0$, los cuales, escritos explícitamente, son respectivamente

$$\begin{bmatrix} -2 & -1 \\ -6 & -3 \end{bmatrix}\begin{bmatrix} s_{11} \\ s_{21} \end{bmatrix} = 0 \quad y \quad \begin{bmatrix} 3 & -1 \\ -6 & 2 \end{bmatrix}\begin{bmatrix} s_{12} \\ s_{22} \end{bmatrix} = 0.$$

Estas ecuaciones nos dan $2s_{11} + s_{21} = 0$ y $3s_{12} - s_{22} = 0$. Escogiendo $s_{11} = 1$ y $s_{12} = 1$, se obtiene $s_{21} = -2$ y $s_{22} = 3$. Por lo tanto, $S = \begin{bmatrix} 1 & 1 \\ -2 & 3 \end{bmatrix}$ y $S^{-1}AS = \begin{bmatrix} 4 & 0 \\ 0 & -1 \end{bmatrix}$

Ejercicios

Encontrar las matrices S no singulares tales que $S^{-1}AS$ sea una matriz en forma diagonal para cada una de las siguientes matrices A:

1. $\begin{bmatrix} 2 & -1 \\ 2 & 5 \end{bmatrix}$. 2. $\begin{bmatrix} 2 & 5 \\ 4 & 1 \end{bmatrix}$. 3. $\begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix}$.

4. $\begin{bmatrix} 1 & 2 & 0 \\ 2 & 1 & 0 \\ 1 & 0 & -3 \end{bmatrix}$. 5. $\begin{bmatrix} 1 & 0 & -1 \\ 2 & 3 & 1 \\ 1 & 0 & 2 \end{bmatrix}$. 6. $\begin{bmatrix} 1 & 1 & -2 \\ 0 & 0 & 5 \\ 4 & 1 & 2 \end{bmatrix}$.

7. Demostrar que toda matriz A de 2×2 tal que $A^2 = -I$ es semejante a la matriz

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

9 Grupos, anillos y campos

1 · SUBGRUPOS NORMALES Y GRUPOS FACTORES

Ahora que se tiene otro ejemplo de una operación no conmutativa, a saber, la multiplicación de matrices, iniciaremos un estudio adicional de las propiedades de los grupos. Es conveniente que el estudiante repase las definiciones de grupo, subgrupo y la de clases laterales derecha e izquierda de un subgrupo en un grupo.

Subgrupo normal o invariante

Sea S un subgrupo de un grupo G. Entonces, si $aS = Sa$ para todo a en G, se dice que S es un subgrupo normal o invariante de G. Obsérvese que, si S es un subgrupo normal de G, las clases laterales derecha e izquierda de S en G coinciden, de manera que puede hablarse de las clases laterales sin ambigüedad.

EJEMPLOS. Todo subgrupo abeliano es un subgrupo normal. El subgrupo S con elementos $i = (1)(2)(3), (123), (132)$ es un subgrupo normal del grupo simétrico de tres símbolos. Las clases laterales derecha e izquierda de este subgrupo en el grupo simétrico de tres símbolos son $i, (123), (132)$ y $(12), (13), (23)$ y de aquí que $aS = Sa$ para todo a en G.

Nótese que, cuando se escribe $aS = Sa$, no se da a entender que debe tenerse $as = sa$ para todos los elementos s de S. Más bien se da a entender que, si se da un elemento s_2 de S tal que $as_1 = s_2a$; s_2 puede ser igual, o no, a s_1. Así se tiene $(12)(123) = (13) = (132)(12)$, donde (123) y (132) están en S.

DEFINICIÓN. Si S_1 y S_2 son dos subconjuntos de un grupo G, se define el *producto* S_1S_2 como el conjunto que consiste de todos los productos s_1s_2 para s_1 en S_1 y s_2 en S_2.

Teorema 1. Si S *es un subgrupo normal de un grupo* G, *entonces el producto,* (aS)(bS), *de dos clases laterales,* aS *y* bS, *de* S *en* G *es la clase lateral* (ab)S.

Si x está en $(ab)S$, entonces $x = (ab)s$, donde s está en S. De aquí que $x = (ai)(bs)$, donde i es el elemento identidad de S. Por lo tanto, x está en $(aS)(bS)$. Recíprocamente, si x está en $(aS)(bS)$, $x = (as_1)(bs_2) = a(s_1b)s_2$, donde s_1 y s_2 están en S. Puesto que S es un subgrupo normal de G, $s_1b = bs_3$, donde s_3 está en S. De aquí que $x = a(bs_3)s_2 = (ab)(s_3s_2)$. Pero S es un subgrupo de G de modo que $s_3s_2 = s_4$ en S. Así, $x = (ab)s_4$ y de aquí que x está en $(ab)S$.

Teorema 2. Si S *es un subgrupo normal de un grupo* G, *entonces las clases laterales de* S *en* G *forman un grupo respecto de la multiplicación de clases laterales.*

Precisamente se ha probado que el producto de dos clases laterales de S es una clase lateral de S. Puede demostrarse fácilmente que $(aS)[(bS(cS)] = [(aS)(bS](cS)$. El elemento identidad es $iS = S$, porque $S(aS) = (Sa)S = (aS)S = a(SS) = aS$ y el inverso de aS es $a^{-1}S$ puesto que $(a^{-1}S)(aS) = (a^{-1}a)(SS) = iS = S$.

EJEMPLO. Las dos clases laterales del subgrupo $i = (1)(2)(3), (123), (132)$ en el grupo simétrico sobre tres símbolos, forma un grupo de orden 2.

Grupo cociente o grupo factor

El grupo de clases laterales de un subgrupo normal S de un grupo G, bajo la multiplicación de clases laterales, se llama grupo cociente o grupo factor del grupo G dado. Se denota por G/S o, en el caso de los grupos abelianos, se acostumbra denotar por $G - S$.

Solamente se pueden usar subgrupos normales para definir un grupo factor de un grupo G. Porque, para que las clases laterales izquierdas o las clases laterales derechas de un subgrupo S en G formen un grupo, se requiere que el producto de dos clases laterales izquierdas de S en G sea una clase lateral izquierda de S o que el producto de dos clases laterales derechas de S sea una clase lateral derecha de S. El teorema siguiente demuestra que esta condición implica que S sea un subgrupo normal.

Teorema 3. Si el producto de dos clases laterales izquierdas de un subgrupo S *en un grupo* G *es una clase lateral izquierda de* S *en* G, *entonces* S *es un subgrupo normal.*

Se desea demostrar que $aS = Sa$ para todo a en G. Primero, se demostrará que todo elemento de Sa es un elemento de aS. Puesto que el producto de dos clases laterales izquierdas es una clase lateral izquierda, se tiene $S(aS) = (iS)(aS) = bS$. Pero $a = i(ai)$ está en $S(aS)$ y, puesto que dos clases laterales son idénticas o ajenas, $bS = aS$. De aquí que $(Sa)S = aS$. Ahora, i está en S y, por lo tanto, si $x = sa$ está en Sa, se tiene $xi = (sa)i = s(ai) = as'$, donde s' está en S, es decir, todo elemento de Sa es un elemento de aS.

Por otra parte, supóngase que as es cualquier elemento de aS, donde s está en S. Fórmese el producto $(as)(a^{-1}s^{-1}) = a(sa^{-1}s^{-1})$. Ya que precisamente se ha demostrado que Sa está contenido en aS, se tiene $sa^{-1} = a^{-1}s_1$, donde s_1 está en S. De aquí que $(as)(a^{-1}s^{-1}) = a(a^{-1}s_1s^{-1}) = a(a^{-1}s_2) = s_2$ está en S ya que S es un subgrupo de G. Se sigue que $as = s_2(sa) = (s_2s)a = s_3a$, donde s_3 está en S. Así, todo elemento, as, de aS es igual a un elemento, s_3a, de Sa y de aquí que $aS = Sa$ para todo a en G.

Ejercicios

1. Probar que las siguientes matrices forman un grupo G respecto de la multiplicación matricial

$$i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad a = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad b = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad c = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$$d = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad e = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad f = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad g = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}.$$

2. En los cuatro ejercicios siguientes denotar por G el grupo del ejercicio 1.
   a. Probar que el subgrupo S que consiste de los elementos i, b es un subgrupo normal de G.
   b. Probar que el grupo factor G/S de G no es cíclico.
   c. Demostrar que los elementos i, a, b, c forman un subgrupo normal de G.
   d. Demostrar que los elementos i, d no forman un subgrupo normal de G.
3. Denotar por k el número de clases laterales izquierdas de un subgrupo S en un grupo G. Probar que, si $k = 2$, el subgrupo S es un subgrupo normal.
4. Probar el teorema 3 para las clases laterales derechas.
5. Probar: Si G es un grupo abeliano y S es un subgrupo de G, entonces G/S es abeliano.
6. Hacer una lista de todos los subgrupos normales del grupo simétrico sobre tres símbolos.

2 · CONJUGADOS

DEFINICIÓN. Sean x y a dos elementos cualesquiera de un grupo G. Entonces, se dice que el elemento $x^{-1}ax$ es el *conjugado* de a bajo G

y $x^{-1}ax$ y a se llaman *elementos conjugados* bajo G. También se dice que el elemento $x^{-1}ax$ es el *transformado* del elemento a por x.

Teorema 4. Los elementos de un grupo pueden separarse en clases mutuamente exclusivas de elementos conjugados.

Para probar este teorema simplemente se necesita demostrar que la relación b conjugado a a bajo un grupo G es una relación de equivalencia. Las tres propiedades de una relación de equivalencia pueden comprobarse de la manera siguiente. El elemento a es conjugado a a porque $i^{-1}ai = a$, donde i es la identidad. Si a es conjugado a b, entonces b es conjugado a a porque, si $a = x^{-1}bx$, entonces $b = xax^{-1} = (x^{-1})^{-1}ax^{-1}$. Si a es conjugado a b y si b es conjugado a c, entonces a es conjugado a c, porque si $a = x^{-1}bx$ y $b = y^{-1}cy$, entonces $a = x^{-1}(y^{-1}cy)x = (yx)^{-1}c(yx)$. Por lo tanto, los elementos de un grupo pueden separarse en clases mutuamente exclusivas de elementos conjugados.

EJEMPLO. El estudiante puede comprobar que los elementos del grupo simétrico sobre tres símbolos pueden separarse en las tres clases siguientes de elementos conjugados. La primera clase consiste de la identidad $i = (1)(2)(3)$; la segunda clase consiste de (123) y (132), y la tercera clase consiste de los elementos (12), (13) y (23).

Teorema 5. Aquellos elementos x *de un grupo* G *tales que* $x^{-1}ax = a$ *forman un subgrupo* N *de* G, *llamado el* **normalizador** *del elemento* a.

Nótese que este teorema dice que todos los elementos de G que son conmutativos con un elemento dado de G, forman un grupo. Es obvio que el normalizador contiene al grupo cíclico generado por el elemento dado. Se procederá a la demostración. Considérese el conjunto N de elementos que son conmutativos con el elemento a. Para probar que N es un subgrupo, simplemente se necesita probar que el conjunto N es cerrado y que si contiene a x contiene a x^{-1}. Sea $x^{-1}ax = a$ y $y^{-1}ay = a$. Entonces, $a = x^{-1}ax = y^{-1}(x^{-1}ax)y = (xy)^{-1}a(xy)$. Por lo tanto, el conjunto N es cerrado. Ahora, si x está en N es obvio que x^{-1} está en N porque, si $x^{-1}ax = a$, $a = xax^{-1} = (x^{-1})^{-1}ax^{-1}$.

Teorema 6. Sea N *el normalizador de un elemento* a *de un grupo* G. *Entonces, todos los elementos de la clase lateral derecha* Nb *de* N *transforman al elemento* a *en el mismo conjugado* $b^{-1}ab$. *Además, si* $b^{-1}ab = c^{-1}ac$, *entonces* Nb = Nc. *Así, existe una correspondencia biunívoca entre las clases laterales derechas de* N *en* G *y los elementos conjugados a* a *bajo* G.

Todo elemento nb de Nb transforma a en $b^{-1}ab$, porque $(nb)^{-1}a(nb) = b^{-1}(n^{-1}an)b = b^{-1}ab$. Ahora, si $b^{-1}ab = c^{-1}ac$, entonces $(bc^{-1})^{-1}a(bc^{-1}) = a$ y bc^{-1} está en N. Ya que bc^{-1} está en N, $N = N(bc^{-1})$ de modo que $Nc = N(bc^{-1})c = Nb(c^{-1}c) = Nb$.

Corolario. Si G *es un grupo finito, el número de elementos en una clase dada de conjugados es un divisor del orden del grupo.*

De acuerdo con el teorema 6, el número de clases laterales derechas distintas del normalizador de un elemento a en G es el número de conjugados en una clase. Ahora, se aplica el teorema de Lagrange que establece que el número de clases laterales derechas de un subgrupo en un grupo, es un divisor del orden del grupo.

Transformación de una permutación

Es interesante encontrar una forma sencilla para transformar cualquier permutación por cualquier otra transformación. Sea $a = (1\,2\,3 \cdots n)$ cualquier ciclo de n símbolos y sea $x = \begin{pmatrix} 1\,2\,3 \cdots n \\ i_1\,i_2\,i_3 \cdots i_n \end{pmatrix}$ cualquier permutación sobre estos n símbolos. Entonces $x^{-1} = \begin{pmatrix} i_1\,i_2\,i_3 \cdots i_n \\ 1\,2\,3 \cdots n \end{pmatrix}$ y fácilmente se ve que $x^{-1}ax = (i_1\,i_2\,i_3 \cdots i_n)$. Así, para transformar la permutación a por cualquier otra permutación, se sustituyen los símbolos en a por los símbolos que les siguen en la permutación de transformación. Sea $a = (123)(456)$ y $x = (2143)(56)$, por ejemplo. Entonces $x^{-1}ax = (412)(365)$.

Subgrupos conjugados

La relación entre conjugados no se restringe a los elementos de un grupo. Si x es un elemento de un grupo G y si S es un subgrupo de G, entonces $x^{-1}Sx$ es un subgrupo de G y se llama conjugado de S bajo G. Fácilmente se ve que $x^{-1}Sx$ es un subgrupo porque el producto de dos elementos del conjunto $x^{-1}Sx$, $(x^{-1}sx)(x^{-1}s'x) = x^{-1}(ss')x$ es otra vez un elemento del conjunto $x^{-1}Sx$. Además, si $x^{-1}sx$ está en $x^{-1}Sx$, entonces su inverso, $x^{-1}s^{-1}x$, está en $x^{-1}Sx$. Por lo tanto, se ve que la palabra subgrupo puede sustituirse por elemento en todos los teoremas precedentes sobre elementos conjugados.

Nótese que la definición de subgrupo normal, es decir, un subgrupo S de G tal que $aS = Sa$ para todo a en G, puede establecerse en una nueva forma diciendo: S es un subgrupo normal de G si $a^{-1}Sa = S$ para todo a en G. Entonces, se dice que un subgrupo normal es *autoconjugado* bajo G.

Ejercicios

1. Separar los elementos del grupo de permutaciones óctuple $i = (1)(2)(3)(4)$, (1234), $(13)(24)$, (1432), (13), (24), $(12)(34)$, $(14)(23)$ en clases de elementos conjugados.
2. Encontrar el normalizador del elemento $(14)(23)$ en el grupo óctuple.
3. Encontrar los subgrupos normales del grupo óctuple.
4. Encontrar las clases de elementos conjugados del grupo cíclico de orden 5.

3 · AUTOMORFISMOS DE UN GRUPO

DEFINICIÓN. Un isomorfismo de un grupo consigo mismo se llama *automorfismo.*

Se desea definir el producto de dos automorfismos de un grupo. Para hacerlo, es conveniente escribir $a \leftrightarrow \mathbf{f}(a)$ en lugar de $a \leftrightarrow a'$, como se hizo anteriormente. Por lo tanto, $\mathbf{f}$ es un automorfismo de un grupo G si y solamente si $a \leftrightarrow \mathbf{f}(a)$ es una correspondencia biunívoca de G consigo mismo y $\mathbf{f}(ab) = \mathbf{f}(a)\mathbf{f}(b)$ para todos los elementos a y b en G.

DEFINICIÓN. El *producto*, $\mathbf{f} \cdot \mathbf{g}$, de dos automorfismos $\mathbf{f}$ y $\mathbf{g}$ de un grupo G, es la correspondencia $\mathbf{h}$ definida por $a \leftrightarrow \mathbf{h}(a) = \mathbf{f}[\mathbf{g}(a)]$.

Ahora, se demostrará que el producto de dos automorfismos es un automorfismo y, de hecho, se probará que se tiene un grupo de automorfismos.

Teorema 7. El conjunto de todos los automorfismos de un grupo forma un grupo bajo la operación producto para los automorfismos.

Sea G un grupo y $\mathbf{f}$, $\mathbf{g}$ y $\mathbf{h}$ automorfismos de G. Entonces, es evidente que $a \leftrightarrow \mathbf{f} \cdot \mathbf{g}(a) = \mathbf{f}[\mathbf{g}(a)]$ es una correspondencia biunívoca entre los elementos de G, puesto que $a \leftrightarrow \mathbf{g}(a) = a'$ y $a' \leftrightarrow \mathbf{f}(a')$ son correspondencias biunívocas. También $\mathbf{f} \cdot \mathbf{g}(ab) = \mathbf{f}[\mathbf{g}(ab)] = \mathbf{f}[\mathbf{g}(a)\mathbf{g}(b)] = \mathbf{f}[\mathbf{g}(a)]\mathbf{f}[\mathbf{g}(b)] = [\mathbf{f} \cdot \mathbf{g}(a)][\mathbf{f} \cdot \mathbf{g}(b)]$ de manera que la correspondencia $a \leftrightarrow \mathbf{f} \cdot \mathbf{g}(a)$ se conserva bajo la operación de grupo. De aquí que es cerrado. Es obvio que, si $\mathbf{i}(a) = a$, la correspondencia $a \leftrightarrow \mathbf{i}(a)$ proporciona el automorfismo identidad $\mathbf{i}$. Si $\mathbf{f}$ es la correspondencia biunívoca $a \leftrightarrow \mathbf{f}(a)$ y $\mathbf{g}$ es la correspondencia biunívoca $\mathbf{f}(a) \leftrightarrow \mathbf{g}[\mathbf{f}(a)] = a$, entonces $\mathbf{g} \cdot \mathbf{f} = \mathbf{i}$ y $\mathbf{g}$ es un inverso izquierdo de $\mathbf{f}$. Finalmente, $[(\mathbf{f} \cdot \mathbf{g}) \cdot \mathbf{h}](a) = [\mathbf{f} \cdot \mathbf{g}]\mathbf{h}(a) = \mathbf{f}\{\mathbf{g}[\mathbf{h}(a)]\} = \mathbf{f}[\mathbf{g} \cdot \mathbf{h}(a)] = [\mathbf{f} \cdot (\mathbf{g} \cdot \mathbf{h})](a)$ de manera que $(\mathbf{f} \cdot \mathbf{g}) \cdot \mathbf{h} = \mathbf{f} \cdot (\mathbf{g} \cdot \mathbf{h})$.

Teorema 8. Para todo elemento fijo $\mathbf{x}$ *de un grupo* $\mathbf{G}$*, la correspondencia* $\mathbf{a} \leftrightarrow \mathbf{x}^{-1}\mathbf{a}\mathbf{x}$ *es un automorfismo de* $\mathbf{G}$.

Si $a \leftrightarrow x^{-1}ax$ y si $b \leftrightarrow x^{-1}bx$, entonces $ab \leftrightarrow (x^{-1}ax)(x^{-1}bx) = x^{-1}(ab)x$.

Los automorfismos que pueden establecerse transformando los elementos de un grupo G por un elemento fijo x de G se llaman automorfismos *internos* de G. Todos los demás automorfismos se llaman automorfismos externos de G.

Teorema 9. Los automorfismos internos de un grupo $\mathbf{G}$ *forman un subgrupo normal* $\mathbf{I}$ *del grupo* $\mathbf{A}$ *de automorfismos de* $\mathbf{G}$.

Sea $\mathbf{f}(a) = x^{-1}ax$ y $\mathbf{g}(a) = y^{-1}ay$. Entonces, $\mathbf{f} \cdot \mathbf{g}(a) = \mathbf{f}(y^{-1}ay) = x^{-1}(y^{-1}ay)x = (x^{-1}y^{-1})a(yx) = (yx)^{-1}a(yx)$. De aquí que $\mathbf{f} \cdot \mathbf{g}$ es un automorfismo interno si $\mathbf{f}$ y $\mathbf{g}$ son automorfismos internos. El automorfismo identidad $\mathbf{i}$ tiene la propiedad de que $\mathbf{i}(a) = a = i^{-1}ai = x$ (donde i es la identidad de G) y de aquí que $\mathbf{i}$ es un automorfismo interno. Finalmente, si $\mathbf{f}(a) = x^{-1}ax$, entonces $\mathbf{f}^{-1}(a) = (x^{-1})^{-1}ax^{-1} = xax^{-1}$ puesto que $\mathbf{f}^{-1} \cdot \mathbf{f}(a) = \mathbf{f}^{-1}(x^{-1}ax) = x(x^{-1}ax)x^{-1} = a = \mathbf{i}(a)$. De aquí que si $\mathbf{f}$ es un automorfismo interno, también lo es $\mathbf{f}^{-1}$. Así, los automorfismos internos forman un subgrupo I del grupo A de automorfismos de G.

Falta por probar que I es un subgrupo normal de A, es decir, debe demostrarse que, si $\mathbf{f}$ es un automorfismo cualquiera y $\mathbf{j}$ es cualquier automorfismo interno, entonces $\mathbf{f}^{-1} \cdot \mathbf{j} \cdot \mathbf{f}$ es un automorfismo interno. Supóngase que $\mathbf{j}(a) = x^{-1}ax$. Entonces

$$
\begin{aligned}
[\mathbf{f}^{-1} \cdot \mathbf{j} \cdot \mathbf{f}](a) &= [\mathbf{f}^{-1} \cdot \mathbf{j}]\mathbf{f}(a) = \mathbf{f}^{-1}[x^{-1}\mathbf{f}(a)x] \\
&= \mathbf{f}^{-1}(x^{-1})\mathbf{f}^{-1}[\mathbf{f}(a)]\mathbf{f}^{-1}(x) = [\mathbf{f}^{-1}(x)]^{-1}a[\mathbf{f}^{-1}(x)] = y^{-1}ay
\end{aligned}
$$

donde $y = \mathbf{f}^{-1}(x)$. (Nótese que puede aplicarse el hecho de que en un isomorfismo, si la imagen de a es b, la imagen de a^{-1} es b^{-1}.)

EJEMPLOS

1. El grupo cíclico de orden cuatro, $a, a^2, a^3, a^4 = i$ no tiene automorfismo interno excepto la identidad, pero tiene los automorfismos externos siguientes:

$$i \leftrightarrow i \qquad a^2 \leftrightarrow a^2$$
$$a \leftrightarrow a^3 \qquad a^3 \leftrightarrow a$$

Por lo tanto, el grupo de automorfismos es de orden 2.

2. El grupo de automorfismos del grupo simétrico sobre tres símbolos consiste solamente de automorfismos internos. Haremos la lista de los automorfismos y bajo cada automorfismo daremos la permutación de transformación x aplicada para establecer el automorfismo:

a	**b**	**c**
$i \leftrightarrow i$	$i \leftrightarrow i$	$i \leftrightarrow i$
$(123) \leftrightarrow (123)$	$(123) \leftrightarrow (132)$	$(123) \leftrightarrow (132)$
$(132) \leftrightarrow (132)$	$(132) \leftrightarrow (123)$	$(132) \leftrightarrow (123)$
$(12) \leftrightarrow (12)$	$(12) \leftrightarrow (13)$	$(12) \leftrightarrow (12)$
$(13) \leftrightarrow (13)$	$(13) \leftrightarrow (12)$	$(13) \leftrightarrow (23)$
$(23) \leftrightarrow (23)$	$(23) \leftrightarrow (23)$	$(23) \leftrightarrow (13)$
$x = i$	$x = (23)$	$x = (12)$

d	**e**	**f**
$i \leftrightarrow i$	$i \leftrightarrow i$	$i \leftrightarrow i$
$(123) \leftrightarrow (132)$	$(123) \leftrightarrow (123)$	$(123) \leftrightarrow (123)$
$(132) \leftrightarrow (123)$	$(132) \leftrightarrow (132)$	$(132) \leftrightarrow (132)$
$(12) \leftrightarrow (23)$	$(12) \leftrightarrow (23)$	$(12) \leftrightarrow (13)$
$(13) \leftrightarrow (13)$	$(13) \leftrightarrow (12)$	$(13) \leftrightarrow (23)$
$(23) \leftrightarrow (12)$	$(23) \leftrightarrow (13)$	$(23) \leftrightarrow (12)$
$x = (13)$	$x = (123)$	$x = (132)$

A continuación, se dará la tabla de multiplicación para el grupo de automorfismos donde **a** es el automorfismo identidad.

	a	**b**	**c**	**d**	**e**	**f**
a	a	b	c	d	e	f
b	b	a	f	e	d	c
c	c	e	a	f	b	d
d	d	f	e	a	c	b
e	e	c	d	b	f	a
f	f	d	b	c	a	e

Por ejemplo:

$$\mathbf{b}\cdot\mathbf{c}(i) = \mathbf{b}[\mathbf{c}(i)] = \mathbf{b}(i) = i = \mathbf{f}(i);$$
$$\mathbf{b}\cdot\mathbf{c}(123) = \mathbf{b}[\mathbf{c}(123)] = \mathbf{b}(132) = (123) = \mathbf{f}(123);$$
$$\mathbf{b}\cdot\mathbf{c}(132) = \mathbf{b}[\mathbf{c}(132)] = \mathbf{b}(123) = (132) = \mathbf{f}(132);$$
$$\mathbf{b}\cdot\mathbf{c}(12) = \mathbf{b}[\mathbf{c}(12)] = \mathbf{b}(12) = (13) = \mathbf{f}(12);$$
$$\mathbf{b}\cdot\mathbf{c}(13) = \mathbf{b}[\mathbf{c}(13)] = \mathbf{b}(23) = (23) = \mathbf{f}(13);$$
$$\mathbf{b}\cdot\mathbf{c}(23) = \mathbf{b}[\mathbf{c}(23)] = \mathbf{b}(13) = (12) = \mathbf{f}(23).$$

Así, $\mathbf{b}\cdot\mathbf{c}(a) = \mathbf{f}(a)$ para todos los elementos a del grupo simétrico sobre tres símbolos y de aquí que $\mathbf{b}\cdot\mathbf{c} = \mathbf{f}$.

Ejercicios

1. Encontrar el orden de cada uno de los automorfismos del grupo simétrico sobre tres símbolos.
2. Encontrar el grupo de automorfismos del grupo de las cinco raíces quintas de la unidad. ¿Es cíclico? ¿Algunos de estos automorfismos son automorfismos internos?
3. Encontrar el grupo de automorfismos del grupo óctuple.
4. Encontrar el grupo de automorfismos del grupo cíclico de orden 6.
5. Encontrar el grupo de automorfismos del grupo cuatro $i = (1)(2)(3)(4)$, $(12)(34)$, $(13)(24)$, $(14)(23)$.
6. Encontrar el grupo de automorfismos del grupo alternante sobre cuatro símbolos. ¿Algunos de los automosfirmos son automorfismos externos?
7. ¿Cuántos automorfismos tiene un grupo cíclico de orden p? ¿Uno de orden pq? (p y q primos distintos).

4 · HOMEOMORFISMOS DE GRUPOS

DEFINICIÓN. Denotemos por $a, b, c, \cdots$, los elementos de un grupo G y por $a', b', c', \cdots$, los elementos de un grupo G'. Se dice que el grupo G' es una imagen *homeomorfa* del grupo G si es posible establecer una correspondencia $a \leftrightarrow a'$ de los elementos de G sobre los elementos de G' tal que:

1. cada elemento a en G' tiene exactamente una imagen a' en G';
2. cada elemento de G' se presenta por lo menos una vez como imagen;
3. si $a \rightarrow a'$ y $b \rightarrow b'$, entonces $ab \rightarrow a'b'$.

La correspondencia se llama *homeomorfismo* de G sobre G'.

Nótese la omisión de la doble flecha para indicar que el mapeo es de G sobre G'. En general, un homeomorfismo no es una correspondencia biunívoca sino una correspondencia múltiple. Si la correspondencia es biunívoca, un homeomorfismo se reduce a un isomorfismo.

EJEMPLO. Sea G el grupo simétrico sobre n símbolos y sea G' el grupo multiplicativo de orden 2 que consiste de los elementos 1 y -1. Puede establecerse un homeomorfismo haciendo que cada permutación para tenga la imagen 1 y cada permutación impar la imagen -1.

Teorema 10. Sea un grupo G' *la imagen homeomorfa de un grupo* G. *Entonces, la imagen de la identidad en* G *es la identidad en* G' *y, si* $\mathrm{a} \rightarrow \mathrm{a}'$, *entonces* $\mathrm{a}^{-1} \rightarrow (\mathrm{a}')^{-1}$.

Este teorema se demuestra en la misma forma en que se demostró el teorema correspondiente para un isomorfismo entre dos grupos. Supóngase que la identidad i de G tiene la imagen a' en el homeomorfismo, y sea x' cualquier elemento de G'. Sea x un elemento de G que tiene x' como imagen en G'. Entonces, $ix \to a'x'$. Sin embargo, $ix = x$ y así, $a'x' = x'$ para todo elemento x' de G. De aquí que a' es la identidad de G'. En forma semejante, si $x^{-1} \to b'$, entonces $x^{-1}x \to b'x'$. Sin embargo, $x^{-1} = i$ y así, $b'x' = i'$, la identidad de G'. Por lo tanto, b' es el inverso de x'.

Ahora, coloquemos en una clase todos aquellos elementos a de G que tienen la misma imagen a' en G'. El teorema siguiente describe estas clases.

Teorema 11. Sea un grupo G' *una imagen homeomorfa de un grupo* G. *Entonces, aquellos elementos* a *de* G *cuya imagen es la identidad en* G' *forman un subgrupo normal* S *de* G *y aquellos elementos de* G *que tienen la misma imagen en* G' *forman una clase lateral de* S *en* G. *El grupo factor* G/S *es isomorfo a* G'.

Considérense los elementos en G que tienen la identidad i' como imagen en G'. Denotemos este conjunto por S. Si $a \to i'$ y $b \to i'$, entonces $ab \to i'i' = i'$. Por lo tanto, el conjunto S es cerrado. Además, si $a \to i'$, entonces, por el teorema previo, $a^{-1} \to (i')^{-1} = i'$ y, así, el inverso de cada elemento en S está en S. De aquí que S es un subgrupo de G.

En seguida se probará que S es un subgrupo normal de G. Ahora, todos los elementos de la clase lateral izquierda xS tienen la misma imagen en G' porque, si $x \to x'$ y s está en S, entonces $xs \to x'i' = x'$. Además, si $y \to x'$, entonces, tal y como se probará, y se encuentra en xS. Ahora, $x^{-1}y \to (x')^{-1}x' = i'$. De aquí que $x^{-1}y$ está en S y y está en xS. En forma semejante, puede probarse que todos los elementos de G, cuya imagen es x' en G', forman la clase lateral derecha Sx. De aquí que $Sx = xS$ y S es un subgrupo normal de G.

Nótese que se ha establecido una correspondencia biunívoca entre las clases laterales de S en G y los elementos a' de G'. De aquí que si $aS \to a'$ y $bS \to b'$, entonces $(aS)(bS) = (ab)S \to a'b'$. De aquí que el grupo factor G/S y G' son isomorfos.

DEFINICIÓN. El subgrupo S se llama *núcleo* del homeomorfismo.

Ahora, combinando la discusión anterior sobre un grupo factor de G con la definición de homeomorfismo, se tiene el siguiente teorema.

Teorema 12. Sea S *un subgrupo normal de un grupo* G. *Entonces, el grupo factor* G/S *es una imagen homeomorfa de* G.

EJEMPLO. Puede establecerse un homeomorfismo del grupo alternante sobre cuatro símbolos sobre el grupo cíclico de orden 3, de la manera siguiente:

$$
\begin{aligned}
i = (1)(2)(3)(4) &\to i' = a^3 \\
(12)(34) &\to i' \\
(13)(24) &\to i' \\
(14)(23) &\to i' \\
(123) &\to a \\
(243) &\to a \\
(142) &\to a \\
(134) &\to a \\
(132) &\to a^2 \\
(143) &\to a^2 \\
(234) &\to a^2 \\
(124) &\to a^2.
\end{aligned}
$$

Ejercicios

1. Establecer un homeomorfismo del grupo óctuple sobre el grupo cíclico de orden 2.
2. Establecer un homeomorfismo del grupo óctuple sobre el grupo de permutaciones $i = (1)(2)(3)(4)$, $(12)(34)$, $(13)(24)$, $(14)(23)$.
3. Establecer un homeomorfismo del grupo cíclico de orden 8 sobre el grupo cíclico de orden 4.
4. Establecer un homeomorfismo del grupo simétrico de cuatro símbolos sobre el grupo simétrico de tres símbolos.
5. Establecer un homeomorfismo del grupo aditivo de los enteros sobre el grupo aditivo de las clases de residuos módulo 3.
6. Establecer un homeomorfismo del grupo aditivo de los enteros sobre el grupo aditivo de las clases de residuos módulo m.
7. Probar que la imagen homeomorfa de un grupo cíclico es un grupo cíclico.

5 · IDEALES EN ANILLOS CONMUTATIVOS

A continuación, se aplicará la teoría de los grupos factores y homeomorfismos de grupos a los anillos conmutativos. Para hacerlo debe definirse un nuevo concepto, a saber, el de un ideal en un anillo conmutativo. Un ideal en un anillo es un cierto tipo de subanillo que desempeña un papel análogo al desarrollado por un subgrupo normal en un grupo. De aquí que, primero, se necesitan las condiciones necesarias y suficientes para que un subconjunto S no vacío de elementos de un anillo R sea un subanillo. Estas son:

1. Los elementos de S forman un subgrupo aditivo del grupo aditivo de R.
2. El conjunto S es cerrado respecto de la multiplicación, es decir, si a y b están en S, entonces ab está en S.

Frecuentemente, la condición (1) se establece de la manera siguiente: si a y b están en S, entonces $a - b$ está en S. El estudiante debe comprobar que ésta es una condición necesaria y suficiente para que un subconjunto no vacío de un grupo sea un subgrupo. Aplicaremos esta formulación de la condición (1) en la definición de un ideal en un anillo conmutativo y, de acuerdo con la costumbre, se denotarán los ideales por letras de tipo "futura".

Definición de un ideal

Un subconjunto de elementos no vacío $\mathbf{m}$ de un anillo conmutativo R es un ideal si se satisfacen las dos condiciones siguientes:

1. Si a y b están en $\mathbf{m}$, entonces $a - b$ está en $\mathbf{m}$.
2. Si a está en $\mathbf{m}$ y si r está en R, entonces ra está en $\mathbf{m}$.

EJEMPLOS.

1. Los enteros pares forman un ideal S en el anillo de los enteros porque, si $2n$ y $2m$ están en S, entonces $2n - 2m = 2(n - m)$ está en S. Además, si r es un entero cualquiera, entonces $r(2n) = 2(rn)$ es un entero par.
2. El anillo R en sí mismo es un ideal llamado *ideal* unitario del anillo.
3. El elemento cero de un anillo es un ideal en el anillo llamado *ideal cero*. Se denota por (0).
4. Sea $R[x]$ el anillo de polinomios con coeficientes enteros. Los polinomios de grado cero (es decir, los enteros) junto con el polinomio cero forman un subanillo de $R[x]$. Sin embargo, este subanillo no es un ideal porque, si $f(x)$ es cualquier polinomio en $R[x]$ de grado mayor que cero y si a es cualquier entero, $af(x)$ no es un entero.
5. El ideal generado por un elemento a de anillo R consiste de todos los elementos de la forma $ra + na$, donde r está en R y n es un entero. Este ideal se llama ideal *principal* y se denota por (a). Se probará que el conjunto de elementos de la forma dada $ra + na$ forman un ideal. Primero, si $r_1a + n_1a$ y $r_2a + n_2a$ están en el conjunto, entonces $r_1a + n_1a - (r_2a + n_2a) = (r_1 - r_2)a + (n_1 - n_2)a$ es de la forma dada. En seguida, sea r cualquier elemento de R. Entonces, $r(r_1a + n_1a) = (rr_1 + n_1r) = r'a + 0 \cdot a$, donde r' está en R. Nótese que, cuando R tiene un elemento unidad u, todo elemento del ideal principal (a) puede escribirse como ra, donde r es un elemento de R. Puesto que un elemento $r'a + na$, donde n es un entero, puede escribirse como $r'a + n(ua) = r'a + (nu)a = (r' + nu)a = ra$ cuando nu es un elemento de R.
6. En forma semejante, se define el ideal $(a_1, a_2, \cdots, a_n)$ en un anillo R generado por el número finito de elementos $a_1, a_2, \cdots, a_n$ de R, como el conjunto de elementos de la forma $\sum_{i=1}^{n} r_ia_i + \sum_{j=1}^{n} n_ja_j$, donde los r_i están en R y los n_j son enteros. Se dice que los elementos $a_1, a_2, \cdots, a_n$ forman una *base* del ideal.

Ejercicios

1. Probar que los múltiplos enteros de cualquier entero fijo m en el anillo de los enteros forman un ideal.
2. En el anillo de los enteros probar que el ideal $(6, 4) = (2)$.
3. En el anillo de los enteros probar que el ideal $(9, 25)$ es el anillo de los enteros.
4. En el anillo de los polinomios $R[x]$, donde R es el anillo de los enteros, probar que todos los polinomios cuyo término constante es cero forman un ideal. ¿Es un ideal principal? Si es así, ¿cuál es su generador?
5. Aplicando el hecho de que todo subgrupo de un grupo cíclico es cíclico, probar que todo ideal en el anillo de los enteros es un ideal principal.
6. Probar que los únicos ideales en el campo de los números racionales son el ideal cero (0) y el propio campo.
7. Probar que los únicos ideales en cualquier campo son el ideal cero y el propio campo.
8. Encontrar todos los ideales en el anillo de las clases de residuos módulo 10.
9. Demostrar que en el anillo polinomial $R[x]$, donde R es el campo de los números racionales, el ideal $(x^2 + 5x + 6, x + 3) = (x + 3)$.
10. Demostrar que todo ideal en el anillo polinomial $F[x]$, donde F es un campo, es un ideal principal. *Sugerencia:* Demostrar que el ideal consiste del ideal cero o contiene un polinomio $r(x)$ de grado tal que todo polinomio en el ideal es un polinomio multiplicado por $r(x)$.

6 · ANILLOS DE CLASES DE RESIDUOS

Los ideales nos permiten construir anillos a partir de un anillo dado, en la misma forma que se construyeron los grupos factores por medio de subgrupos normales. Puesto que un ideal $\mathbf{m}$ en un anillo conmutativo R es un subgrupo normal del grupo aditivo del anillo, los elementos del anillo pueden separarse en clases laterales de $\mathbf{m}$ en R. Estas clases laterales se llaman clases de residuos de R cuyo módulo es el ideal $\mathbf{m}$. Así, una clase de residuos módulo $\mathbf{m}$ es el conjunto de elementos $\mathbf{m} + a$, donde a es cualquier elemento del anillo R. Recuérdese que una condición necesaria y suficiente para la igualdad de dos clases laterales Sa y Sb de un subgrupo S en un grupo G es que ab^{-1} esté en S. (Ver pág. 76, ejercicio 6). Esta condición, traducida a la notación aditiva y aplicada como un criterio para la igualdad de dos clases de residuos $\mathbf{m} + a$ y $\mathbf{m} + b$, es que $a - b$ esté en $\mathbf{m}$. Así, se tiene una generalización de la idea de las congruencias de los enteros. Se probarán las siguientes reglas que gobiernan las congruencias cuyo módulo es un ideal $\mathbf{m}$.

Teorema 13. Sea R *un anillo conmutativo y* $\mathbf{m}$ *un ideal en* R. *Si* $a \equiv b \ (mod\ \mathbf{m})$ *y si* $a' \equiv b' \ (mod\ \mathbf{m})$, *entonces* $a + a' \equiv b + b' \ (mod\ \mathbf{m})$, $aa' \equiv bb' \ (mod\ \mathbf{m})$ *y* $ra \equiv rb \ (mod\ \mathbf{m})$, *donde* r *está en* R.

Puesto que tanto $a - b$ como $a' - b'$ están en $\mathbf{m}$, entnoces, $(a - b) + (a' - b') = (a + a') - (b + b')$ está en $\mathbf{m}$ y $a + a' \equiv b + b'$ (mod $\mathbf{m}$). Además, ya que $a - b$ está en $\mathbf{m}$, $a'(a - b)$ está en $\mathbf{m}$ y puesto que $a' - b'$ está en $\mathbf{m}$, $(a' - b')b$ está en $\mathbf{m}$. Por lo tanto, $a'(a - b) + (a' - b')b = a'a - b'b$ está en $\mathbf{m}$ y $a'a \equiv b'b$ (mod $\mathbf{m}$). Es obvio que, si $a - b$ está en $\mathbf{m}$, $r(a - b)$ está en b y $ra \equiv rb$ (mod $\mathbf{m}$).

Definición de adición y multiplicación de clases de residuos

Sea a un elemento de la clase de residuos $\mathbf{m} + a$ y b un elemento de la clase de residuos $\mathbf{m} + b$. La *suma* de las dos clases de residuos $\mathbf{m} + a$ y $\mathbf{m} + b$ se define como la clase que contiene al elemento $a + b$. El *producto* de dos clases de residuos $\mathbf{m} + a$ y $\mathbf{m} + b$ se define como la clase de residuos que contiene al producto ab. Obsérvese que, de acuerdo con el teorema anterior, la clase de residuos suma y la clase de residuos producto, son independientes de los elementos representativos particulares que se hayan escogido de las clases de residuos dadas.

Teorema 14. Sea R *anillo conmutativo y* $\mathbf{m}$ *un ideal en* R. *Las clases de residuos módulo* $\mathbf{m}$ *forman un anillo respecto de la adición y la multiplicación.*

El anillo formado por las clases de residuos módulo $\mathbf{m}$ se llama *anillo de clase de residuos* denotado por $R - \mathbf{m}$.

De la teoría de grupos se sabe que las clases de residuos forman un grupo abeliano aditivo puesto que son conjuntos laterales de un subgrupo normal $\mathbf{m}$ en un grupo abeliano aditivo R. La definición anterior. de producto de dos clases de residuos nos proporciona la cerradura respecto de la multiplicación. Se deja al estudiante la demostración de las leyes asociativas para la multiplicación y la ley distributiva.

EJEMPLOS.

1. Sea R el anillo de los enteros y $\mathbf{m} = (m)$. Entonces, $R/(m)$ es el anillo de las clases de residuos cuyo módulo es el entero m.

2. Sea $R[x]$ el anillo polinomial, donde R es el anillo de los enetros y $\mathbf{m}$ el ideal $(x - 3)$. El ideal $(x - 3)$ consiste de todos los elementos de la forma $f(x)(x - 3)$, donde $f(x)$ es un polinomio en $R[x]$. Ahora, cualquier polinomio $g(x)$ en $R[x]$ puede escribirse como $g(x) = q(x)(x - 3) + g(3)$. Por lo tanto, $g(x) \equiv g(3)$ (mod $(x - 3)$). Es decir, cualquier clase de residuos puede representarse por un entero. Ahora, si dos enteros a y b se encuentran en la misma clase de residuos, $a - b$ está en el ideal $(x - 3)$, esto es, $a - b \equiv q(x)(\ - 3)$. Ahora, a menos que $q(x) = 0$, el grado del segundo miembro es mayor que cero. De aquí que $q(x) = 0$ y $a = b$. Por lo tanto, cada entero determina una clase de residuos diferente. De aquí que pueda establecerse una correspondencia

biunívoca entre las clases de residuos de $R[x]$ módulo $(x - 3)$ y los enteros a haciendo $(x - 3) + a \leftrightarrow a$. El estudiante puede comprobar fácilmente que esta correspondencia es un isomorfismo.

3. Sea R el anillo de los números complejos $a + bi$, donde a y b son enteros y sea $\mathbf{m} = (2)$. Entonces, ya que 2 y $2i$ son elementos de $\mathbf{m}$, cualquier número $a + bi = 2k + r + (2k' + r')i$, donde $0 < r \leq 2$ y $0 \leq r' < 2$. Así, $a + bi \equiv r + r'i$ (mod (2)). De aquí que se tienen las cuatro distintas clases de residuos: (2), (2) + 1, (2) + i, (2) + 1 + i.

Ejercicios

1. Determinar si las clases de residuos del ejemplo 3 forman un dominio entero.
2. Presentar el anillo de clases de residuos del anillo de los números complejos de la forma $a + bi$, donde a y b son enteros, cuyo módulo es el ideal (3). ¿Es un campo este anillo de clases de residuos?
3. Presentar el anillo de clases de residuos del anillo $R[x]$, donde R es el anillo de los enteros cuyo módulo es el ideal (x).
4. Presentar el anillo de clases de residuos del anillo $R[x]$, donde R es el anillo de los enteros cuyo módulo es el ideal $(x^2 + 1)$.
5. Probar las leyes asociativas para la multiplicación y la ley distributiva en $R/(m)$.

7 · HOMEOMORFISMOS DE ANILLOS

La definición de homeomorfismo de un anillo es una extensión de la definición de homeomorfismo de un grupo. La correspondencia simplemente asegura dos operaciones en lugar de una.

DEFINICIÓN. Denotemos por $a, b, c, \cdots$ los elementos de un anillo R y por $a', b', c', \cdots$ los elementos de un anillo R'. Se dice que el anillo R' es una *imagen homeomorfa* del anillo R si es posible establecer una correspondencia $a \rightarrow a'$ de los elementos de R sobre los elementos de R' tal que:

1. Cada elemento a en R tiene exactamente una imagen a' en R';
2. Cada elemento de R' se presenta por lo menos una vez como imagen;
3. Si $a \rightarrow a'$ y $b \rightarrow b'$, entonces $a + b \rightarrow a' + b'$ y $ab \rightarrow a'b'$.

Una vez más se observa que un homeomorfismo es un mapeo múltiple de los elementos de R en los elementos de R'. Se demostrará la relación íntima entre los ideales y los homeomorfismos de los anillos en el siguiente teorema.

Teorema 15. Si un anillo R' *es una imagen homeomorfa de un anillo conmutativo* R, *aquellos elementos de* R *cuya imagen es el ele-*

mento cero de R′ *forman un ideal* **m**, *y el anillo de clases de residuos* R/**m** *es isomorfo a* R′.

Primero, se demostrará que aquellos elementos de R cuya imagen es el elemento cero de R' forman un ideal **m**. Denotemos el elemento cero de R' por $0'$. Entonces, si $a \to 0'$ y $b \to 0'$, se tiene $a - b \to 0' - 0' = 0'$. Además, si r es cualquier elemento del anillo R cuya imagen es r' en R', $ra \to r' \cdot 0' = 0'$. Por lo tanto, aquellos elementos de R cuya imagen es el elemento cero de R' forman un ideal **m** en R. A continuación, separemos los elementos de R en clases de residuos módulos **m**. Si $a \to a'$, todos los elementos de la clase de residuos $\mathbf{m} + a$ tienen la imagen a', pues todo elemento $m + a$, donde m está en **m** de esta clase, se mapea en $0' + a' = a'$. Además, si $b \to a'$, entonces $a - b \to a' - a' = 0'$ y $a - b$ está en **m**. Si ahora se consideran las clases de residuos de R módulo **m** como elementos, es obvio que la correspondencia $\mathbf{m} + a \to a'$ es un isomorfismo porque si $\mathbf{m} + b \to b'$, entonces $\mathbf{m} + a + b \to a' + b'$ y $\mathbf{m} + ab \to a'b'$.

Ahora, combinando nuestra discusión previa sobre los anillos de clases de residuos de un anillo R con la definición de homeomorfismo, puede verse que cualquier anillo de clases de residuos de R es una imagen homeomorfa de R. Sea **m** un ideal en R, entonces la correspondencia $a \to \mathbf{m} + a$ nos da el homeomorfismo. De aquí que se tiene el teorema siguiente.

Teorema 16. Todo ideal **m** *en un anillo conmutativo* R *determina un homeomorfismo de* R *en su anillo de clases de residuos* R/**m**.

Ejercicios

1. Probar que una imagen homeomorfa de un anillo conmutativo es un anillo conmutativo.
2. Probar que, si R' es una imagen homeomorfa de un anillo R con elemento unidad, R' tiene un elemento unidad.
3. ¿Cuáles son las imágenes homeomorfas posibles de un campo?
4. El anillo polinomial $F[x]$, donde F es el campo de los números racionales, se mapea homeomorfamente en el anillo de los números complejos $a + bi$, donde a y b son racionales, mediante la correspondencia $f(x) \to f(i)$. ¿Cuál es el ideal que determina el homeomorfismo?
5. Encontrar todos los ideales en el anillo de clases de residuos de los enteros módulo 12. De aquí, encontrar todas las imágenes homeomorfas de este anillo de clases de residuos.

8 · AUTOMORFISMOS DE CAMPOS

Automorfismo de un campo

Un automorfismo de un campo F es una correspondencia biunívoca de F consigo mismo que se conserva bajo la adición y la multiplicación.

En términos de la notación introducida en relación con los automorfismos de grupos, **f** es un automorfismo de un campo F si es una correspondencia biunívoca de F consigo mismo tal que $\mathbf{f}(a + b) = \mathbf{f}(a) + \mathbf{f}(b)$ y $\mathbf{f}(ab) = \mathbf{f}(a)\mathbf{f}(b)$.

EJEMPLOS.

1. Si $a \leftrightarrow a$ se tiene el automorfismo *identidad*.

2. Sea F el campo que consiste de todos los números de la forma $a + b\sqrt{2}$, donde a y b son números racionales. Entonces $a + b\sqrt{2} \leftrightarrow a - b\sqrt{2}$ es un automorfismo de F. Puesto que si $a + b\sqrt{2} \leftrightarrow a - b\sqrt{2}$ y $c + d\sqrt{2} \leftrightarrow c - d\sqrt{2}$, entonces $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \leftrightarrow (a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2})$ y $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \leftrightarrow (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2})$.

3. Si F es el campo de los números reales, la correspondencia $a \leftrightarrow -a$ es biunívoca y se conserva bajo la adición pero no se conserva bajo la multiplicación. Porque $a + b \leftrightarrow -(a + b) = (-a) + (-b)$ pero $ab \leftrightarrow -(ab) \neq (-a)(-b)$. De aquí que esta correspondencia no es un automorfismo.

4. Puede aplicarse el concepto de automorfismo de un campo para proporcionar una demostración alternativa del teorema 12 del capítulo 5. Si $a_0x^n + a_1x^{n-1} + \cdots + a_n$, donde $a_0, a_1, \cdots a_n$ son números reales, tiene el cero $a + bi$, (a y b son números reales) se tiene $a_0(a + bi)^n + a_1(a + bi)^{n-1} + \cdots + a_n = 0$. Ahora, considérese el automorfismo **f** del campo de los números complejos definido por $\mathbf{f}(a + bi) = a - bi$ para a y b números reales. Entonces

$$\begin{aligned}&\mathbf{f}[a_0(a + bi)^n + a_1(a + bi)^{n-1} + \cdots + a_n]\\ &= \mathbf{f}(a_0)[\mathbf{f}(a + bi)]^n + \mathbf{f}(a_1)[\mathbf{f}(a + bi)]^{n-1} + \cdots + \mathbf{f}(a_n)\\ &= a_0(a - bi)^n + a_1(a - bi)^{n-1} + \cdots + a_n = \mathbf{f}(0) = 0.\end{aligned}$$

Las demostraciones de los teoremas siguientes son muy semejantes a las demostraciones de los teoremas correspondientes para los grupos y se dejan como ejercicios para el estudiante.

Teorema 17. Si **f** *es un automorfismo de un campo* F *con identidad aditiva* 0 *e identidad multiplicativa* 1, $\mathbf{f}(0) = 0$ *y* $\mathbf{f}(1) = 1$.

Teorema 18. Sean **f** *y* **g** *automorfismos de un campo* F. *Entonces, la correspondencia* **k** *dada por* $a \leftrightarrow \mathbf{k}(a) = \mathbf{f}[\mathbf{g}(a)]$ *es un automorfismo de* F.

EJEMPLO. Sea F el campo que consiste de los números $a + b\sqrt{2} + ci + d\sqrt{2i}$, donde a, b, c y d son números racionales. Entonces, si $\mathbf{f}(a + b\sqrt{2} + ci + d\sqrt{2i}) = a - b\sqrt{2} + ci - d\sqrt{2i}$ y $\mathbf{g}(a + b\sqrt{2}i + ci + d\sqrt{2i}) = a + b\sqrt{2} - ci - d\sqrt{2i}$, $\mathbf{f}$ y $\mathbf{g}$ son automorfismos de F. Entonces, $\mathbf{k}$ se define por $\mathbf{k}(a + b\sqrt{2} + ci + d\sqrt{2}i = \mathbf{f}[\mathbf{g}(a + b\sqrt{2} + ci + d\sqrt{2i})] = \mathbf{f}(a + b\sqrt{2} - ci - d\sqrt{2i}) = a - b\sqrt{2} - ci + d\sqrt{2}i$ y es otro automorfismo de F.

DEFINICIÓN. Si $\mathbf{f}$ y $\mathbf{g}$ son automorfismos de un campo F, $\mathbf{f} \cdot \mathbf{g}$ es el automorfismo $\mathbf{k}$ definido por $a \leftrightarrow \mathbf{k}(a) = \mathbf{f}[\mathbf{g}(a)]$.

Teorema 19. El conjunto de todos los automorfismos de un campo F *forman un grupo llamado grupo de automorfismos de* F.

Regresemos al ejemplo que sigue del teorema 18. Puede demostrarse que los únicos automorfismos de este campo son el automorfismo identidad $\mathbf{e}$ y los automorfismos $\mathbf{f}$, $\mathbf{g}$ y $\mathbf{k}$. El grupo de automorfismos de F tiene la tabla de multiplicación

	e	**f**	**g**	**k**
e	**e**	**f**	**g**	**k**
f	**f**	**e**	**k**	**g**
g	**g**	**k**	**e**	**f**
k	**k**	**g**	**f**	**e**

Ejercicios

1. Probar el teorema 17.
2. Probar el teorema 18.
3. Probar el teorema 19.
4. Considérese el campo F que consiste de todos los números de la forma $a + br + cr^2 + dr^3 + ei + fir + gir^2 + hir^3$, donde $a, b, \cdots, h$ son números racionales y $r = \sqrt[4]{3}$. Encontrar todos los automorfismos $\mathbf{f}$ de F tales que $\mathbf{f}(i) = i$.

Bibliografía

REFERENCIAS GENERALES

ALBERT, A. A., *Introduction to Algebraic Theories*, Chicago, University of Chicago Press, 1941.

ALBERT, A. A., *Modern Higher Algebra*, Chicago, University of Chicago Press, 1937.

ANDREE, R. V., *Selections from Modern Abstract Algebra*, Nueva York, Henry Holt and Co., 1958.

BIRKHOFF, G., y S. MACLANE, *A Survey of Modern Algebra*, edición revisada, Nueva York, The Macmillan Co., 1953.

JOHNSON, R. E., *First Course in Abstract Algebra*, Englewood Cliffs, N. J., Prentice Hall, 1953.

MCCOY, N. H., *Introduction to Modern Algebra*, Boston, Allyn and Bacon, 1960.

MACDUFFEE, C. C., *An Introduction to Abstract Algebra*, Nueva York, John Wiley and Sons, 1940.

VAN DER WAERDEN, B. L., *Modern Algebra*, vols. 1 y 2, traducidos del alemán al inglés por Fred Blum, Nueva York, Frederic Unger Publishing Co., 1953.

TEORIA DE NUMEROS

DICKSON, L. E., *Modern Elementary Theory of Numbers*, Chicago, University of Chicago Press, 1939.

ORE, O., *Number Theory and Its History*, Nueva York, McGraw-Hill Book Co., 1952.

NIVEN I, y H. S. ZUCKERMAN, *Introduction to the Theory of Numbers*, Nueva York, John Wiley and Sons, 1960.

STEWART, B. M, *Theory of Numbers*, Nueva York, The Macmillan Co., 1952.

USPENSKY, J. V. y M. H. HEASLET, *Elementary Number Theory*, Nueva York, McGraw-Hill Book Co., 1939.

TEORIA DE GRUPOS

CARMICHAEL, R. D., *Introduction to the Theory of Groups of Finite Order*, Nueva York, Dover Publications, 1956.

HALL, M., JR., *The Theory of Groups*, Nueva York, The Macmillan Co., 1959.

KUROSH, A. G., *The Theory of Groups*, vol. 1, traducido del ruso por K. A. Hirsch, Nueva York, Chelsea Publishing Co., 1949.

VECTORES Y MATRICES

HALMOS, P. R., *Finite Dimensional Vector Spaces*, 2ª edición, Princeton, N. J., D. Van Nostrand Co., 1958.
HOHN, F. E., *Elementary Matrix Algebra*, Nueva York, The Macmillan Co., 1958.
MACDUFFEE, C. C., *The Theory of Matrices*, 2ª edición, Nueva York, Chelsea Publishing Co., 1946.
MACDUFFEE, C. C., *Vectors and Matrices*, Carus Mathematical Monograph Nº 7, Buffalo, N. Y., The Mathematical Association of America, 1943.
MURDOCH, D. C., *Linear Algebra for Undergraduates*, Nueva York, John Wiley and Sons, 1957.
PERLIS, S., *Theory of Matrices*, Cambridge, Mass., Addison-Wesley Press, 1952.
STOLL, R. R., *Linear Algebra and Matrix Theory*, Nueva York, McGraw-Hill Book Co., 1952.
THRALL, R. M. y L. TORNHEIM, *Vector Spaces and Matrices*, Nueva York, John Wiley and Sons, 1957.

ANILLOS E IDEALES

ARTIN, E., C. J. NESBITT y R. M. THRALL, *Rings with Minimum Condition*, Ann Arbor, University of Michigan Press, 1944.
JACOBSON, N., *The Theory of Rings*, Mathematical Surveys, Nº 2, Nueva York, American Mathematical Society, 1943.
McCOY, N. H., *Rings and Ideals*, Carus Mathematical Monograph Nº 8, Buffalo, Nueva York., The Mathematical Association of America, 1948.

Indice alfabético

SE TERMINO DE IMPRIMIR ESTA OBRA EL DIA 28 DE JUNIO DE 1967, EN LOS TALLERES DE *UNION GRAFICA, S. A.*, AV. DIVISION DEL NORTE, 1521 MEXICO 13, D. F. LA EDICION CONSTA DE 3 000 EJEMPLARES MAS SOBRANTES PARA REPOSICION.

EJEMPLAR Nº 0320